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

Monthly Security Bulletin

December 2018/January 2019

Table of Contents

Executive summary.......2

1. Amazon Sends 1,700 Alexa Voice Recordings to a Random Person.......3

2. in(Secure) messaging apps — How side-channel attacks can compromise privacy in WhatsApp, Telegram, and Signal.......4

3. Hidden Code in Memes Instruct Malware via Twitter.......14

4. Facebook Flaw Exposes Private Photos for 6.8M Users.......16

5. Biometrics: Security Solution or Issue?.......17

6. KoffeyMaker: notebook vs. ATM.......18

7. Netbooks, RPis, & Bash Bunny Gear - Attacking Banks from the Inside.......19

8. The Ransomware Doctor Without A Cure.......21

9. Logitech Keystroke Injection Flaw Went Unaddressed for Months.......25

10. Remote Firmware Attack Renders Servers Unbootable.......26

11. 123456 Is the Most Used Password for the 5th Year in a Row.......29

Executive summary

The below Monthly Security bulletin is collection of tsome of the hottest IT news and events of December 2018 and will cover in a greater detail the following topics:

- Amazon has sent 100MB ZIP file containing personal data, including 1700 audio files, of a customer to a random person. The tech giant says this is a one-time mishap due to an employee's mistake. Only after investigative reporters got involved and found the real customer Amazon has spoken on the matter. Jump to article
- With the growing concern about privacy more and more people are installing apps offering end-to-end encryption for secure instant messaging that keep their content secure from any third parties. However, after taking deep dive look, they might not be as secure as they claim to be. This article takes a closer look into 3 of the most popular apps on the market: WhatsApp, Telegram and Signal. *Jump to article*
- Memes are no longer just funny, satirical images with text. They are being used to spread hidden embedded code in them via Twitter. *Jump to article*
- Facebook is in hot water again. Recently exposed flaw in their system allows third-party apps to gain access to the unposted "draft" photos of 6.7 million users. *Jump to article*
- "With more transactions occurring online – and subsequently, the number of data breaches increasing – biometrics are moving to the forefront in discussions as a top way to authenticate data securely. However, challenges remain." *Jump to article*
- Low cost, black box attacks on ATMs are on the rise. Kaspersky Lab' experts have investigated the KoffeyMaker tool and how easily it can be used. *Jump to article*
- "Multiple banks in Eastern Europe have been attacked from inside their network via various electronic devices connected directly to the company's own infrastructure, security researchers have discovered." *Jump to article*
- With the rise of ransomware attacks, it is only normal to have the surge in IT consultancy services offerings. However, victims of ransomware have to be cautions who they hire to help with the problem. Companies like Dr. Shifro offer services too good to be true… And they are, the company simply acts as broker between the victim and the attacker. *Jump to article*
- "Computer peripheral giant Logitech has finally issued a patched version of its Logitech Options desktop app, after being taken to task for a months-old security flaw. The bug could have allowed adversaries to launch keystroke injection attacks against Logitech keyboard owners that used the app." *Jump to article*
- "Security researchers have found a way to corrupt the firmware of a critical component usually found in servers to turn the systems into an unbootable hardware assembly. The recovery procedure requires physical intervention to replace the malicious firmware." *Jump to article*
- Bad habits die hard, apparently so do predictable, easily guessable passwords as well. SplashData's eighth annual list of Worst Passwords of the Year shows that "123456" is the most used password for 5th consecutive year. If you what to know what the top 10 most used passwords are and "Worst Password Offenders" *Jump to article*

1. Amazon Sends 1,700 Alexa Voice Recordings to a Random Person

The intimate recordings paint a detailed picture of a man's life.

Amazon inadvertently sent 1,700 audio files containing recordings of Alexa interactions by a customer to a random person – and after a newspaper investigation exposed the snafu, characterized it as a "mishap" that came down to one employee's mistake.

In August, an Amazon customer in Germany (going by the alias "Martin Schneider" for purposes of the report) made use of his rights under the recently passed EU General Data Protection Regulation (GDPR) to ask for copies of the personal data Amazon has on file about him.

Amazon complied, sending Schneider a 100MB ZIP file which, among other things, contained about 1,700 Alexa audio files along with transcripts of Alexa voice commands. There was just one problem – Schneider doesn't use Alexa. After listening to a few of the files, they were clearly of someone else speaking, so he concluded that Amazon sent him the data in error. But Amazon didn't respond to his efforts to contact them about the problem, he said, so he contacted Heise Media's c't publication in mid-November.

The shocking part of the story is how quickly the investigative reporters were able to identify the victim. From the recordings, which cover the entire month of May 2018, they were able to determine that he has a Fire TV and an Echo box, and that he uses Alexa to control a smart home thermostat as well as his phone. A female voice speaking to Alexa indicates that he has also a female companion. They were also able to hear the man in the shower while he was issuing certain commands. There were also alarms, Spotify commands, public transport and weather inquiries.

"We were able to navigate around a complete stranger's private life without his knowledge, and the immoral, almost voyeuristic nature of what we were doing got our hair standing on end," the investigators noted in their report, published on Thursday.

They were further able to identify and track down the victim via Twitter.

"Using these files, it was fairly easy to identify the person involved and his female companion; weather queries, first names, and even someone's last name enabled us to quickly zero in on his circle of friends," according to the report. "Public data from Facebook and Twitter rounded out the picture."

Needless to say, the victim was shocked. He said that he too had filed an information request – clearly there was a mix-up. The investigators notified Amazon of the data breach, to which it responded that the situation was an "unfortunate mishap" and a one-time error. Amazon called both of the impacted customers as well.

A spokesperson for the tech giant told us: “This was an unfortunate case of human error and an isolated incident. We have resolved the issue with the two customers involved and have taken steps to further improve our processes. We were also in touch on a precautionary basis with the relevant regulatory authorities.”

This isn’t the first time Amazon Alexa has presented privacy issues. Earlier this year a family in Portland, Ore. said their Echo device recorded their conversation and sent it to a random person on their contact list. And researchers have uncovered more than one way to hack Alexa devices in order to eavesdrop on people. This however may be the first publicized instance of a manual, human error resulting in an issue for the voice-recognition technology.

“This news isn’t a big surprise to me,” Boris Cipot, senior sales engineer at Synopsys said, via email. “If I recall correctly, Amazon also uses voice data for learning purposes to make its voice AI better. The Alexa App used to also show you the transcript of all the questions you have asked it, where you could also give your feedback as to whether it was handled correctly or not. As this data is then stored somewhere for ‘learning’ purposes, this then also poses the risk that if the data is not handled correctly it could have bad consequences.”

The recording of Alexa interactions (and the practice of keeping them in the cloud) is indeed necessary to improve the platform over time, according to Amazon; the company also allows users to review and delete voice recordings, according to its data privacy FAQ.

“The inner workings of Amazon are a mystery,” Cipot added. “Even if they would like to have more transparency, they also need to keep some secrets for the sake of security and also company secrets of how they do things. Every company (be it Amazon, Google, Apple…) has those secrets, and every smart device (be it Echo, a Smartphone or even a TV) have the same functionalities that we don’t know all the inner workings of, along with the data they collect and store.”

Source: https://threatpost.com/amazon-1700-alexa-voice-recordings/140201/

2. in(Secure) messaging apps — How side-channel attacks can compromise privacy in WhatsApp, Telegram, and Signal

Messaging applications have been around since the inception of the internet. But recently, due to the increased awareness around mass surveillance in some countries, more users are installing end-to-end encrypted apps dubbed "secure instant messaging applications." These apps claim to encrypt users' messages and keep their content secure from any third parties.

However, after a deep dive into three of these secure messaging apps — Telegram, WhatsApp and Signal — we discovered that these services may not fulfill the promises they are meant to keep by putting users' confidential information at risk.

This is a serious problem, considering users download these apps in the hopes that their photos and messages will stay completely protected from third parties. These apps, which have countless users, cannot assume that their users are security educated and understand the risk of enabling certain settings on their device. As such, they have an obligation to explain the risks to users, and when possible, adopt safer defaults in their settings

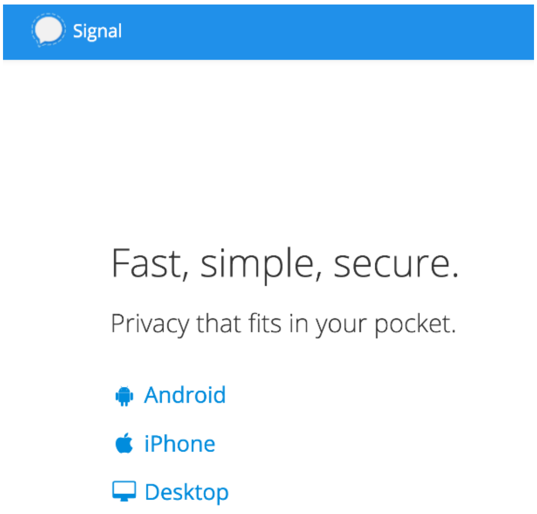
Secure messaging applications

The concept behind secure messaging apps is that the content of all communication is encrypted between users without third parties involved. This means the service provider should not be able to read the content at any point.

To achieve end-to-end encryption, these applications either developed their own cryptographic protocol or adopted a third-party one. There are two main protocols these apps usually use: MT Protocol developed by the secure messaging app Telegram, and Signal Protocol, developed by the software firm Open Whisper Systems. Since MT Protocol implementation is not open-source, most of the remaining applications either use Signal Protocol or implemented a variation of it. Other applications, which are beyond the scope of this post, use this protocol upon request from the user, but not by default. That is the case of both Facebook Messenger, which utilizes a feature known as "Secret Conversations" and Google Allo, which has a feature called "Incognito" chats. In both protocols, the cryptographic implementation has been highly scrutinised by the security community. Researchers in the past have analyzed publicly available source code and performed black-box analysis in real-time communication data.

However, a secure messaging application is much more than the cryptographic protocol. There are other components, such as the UI framework, file storage model, group enrollment and mechanisms that could all be used as an attack vector. The vulnerability CVE 2018-1000136 found in the Electron framework, which is used by both WhatsApp and Signal to build their user interface, is a good example of this. This vulnerability, in a worst case scenario, could allow an attacker to execute code remotely or could be used to copy messages.

These protocols are focused on keeping communications private while in transit. However, they usually provide no assurances about security while the data is processing or when the message reaches the user's device. These protocols also don't manage group enrollment on these applications, as evidenced by the recent vulnerability found in WhatsApp. If an attacker compromises a WhatsApp server, they could add new members to a group without the group administrator's approval, allowing them to read new messages. This means there's the potential for a motivated actor to pick and choose specific WhatsApp groups to eavesdrop on, breaking the common understanding that this application provides bulletproof end-to-end encryption on all communications.



Signal

Fast, simple, secure.

Privacy that fits in your pocket.

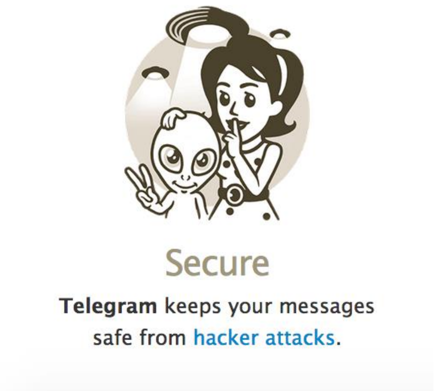
- Android
- iPhone
- Desktop

Figure 1. A presentation from Signal pledges to keep users' messages secure.
Source: http://www.signal.org

Behind the technical aspects of these applications is also an essential human aspect.

All of these applications advertise themselves as secure and privacy-minded. Some of them even go as far as to state that they are "safe from hacker attacks." All these statements are meant to create trust between the users and the application. Users trust that the applications will keep their private data safe.

Given that all of these applications claim to have millions of active users, it is clear that not all of these users will be cyber security-educated. As such, most of them won't have a full understanding of the risks and limitations posed by certain configurations on these applications. Keeping a person's privacy safe is more than just technology, it's also about providing the users with the correct information in a manner that they are able to understand the risks of their decisions, even without being security experts.



Secure

Telegram keeps your messages safe from hacker attacks.

Figure 2. A Telegram advertisement states that it will keep users' messages "safe from hacker attacks."
Source: http://www.telegram.com

Another significant feature that is advertised on these apps is their multi-platform capability. All apps support the major mobile device platforms and a desktop version. The typical user will rightfully believe that the security level is the same on all platforms. All the applications' websites present the idea that the security, privacy and platforms are kept at the same level.

Implementing security features tends to vary between these various platforms. Some platforms have more risks than others and these risks need to be communicated to the users since they will usually assume that each platform provides the same level of security protection.

The problem

The majority of these applications' users are not cybersecurity educated, which means they blindly trust these applications to keep their information safe and secure. It is clear that the source of such trust is the way the applications advertise their services.

On May 16, 2018, Talos published an article on Telegrab, a malware that can hijack sessions from Telegram. The concept is simple: If an attacker can copy the session tokens from a desktop user, then it will be able to hijack the session. The attacker won't need anything else other than the information that is stored locally. It doesn't matter if the information is encrypted or not — by copying this information, the attacker will be able to use it to create a shadow session.

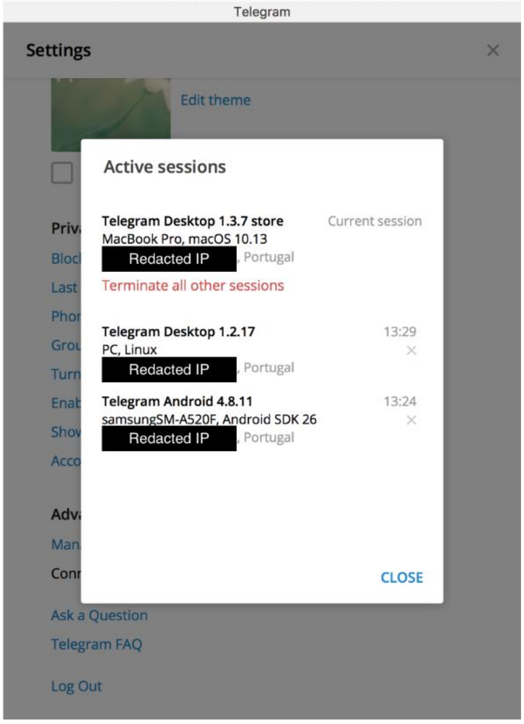
Following up on that research, we decided to check if the same technique was also applicable to other messaging applications, which was proven to be correct on all tested applications (Telegram, Signal, WhatsApp). Not all of these applications handled sessions in the same way, which leads to different consequences upon this attack.

In the next section, we will describe some of these attack scenarios where the sessions of these applications can be replicated or hijacked.

APPLICATIONS

Telegram — Desktop session hijacking

Telegram seems to be the application where session hijacking is most likely to happen without users having any kind of indication that the attack occurred. Messages and images that are sent or received by the victim are replicated into the attacker's session.



Telegram

Settings

Edit theme

Active sessions

Telegram Desktop 1.3.7 store — Current session
MacBook Pro, macOS 10.13
Redacted IP, Portugal

Terminate all other sessions

Telegram Desktop 1.2.17 — 13:29
PC, Linux
Redacted IP, Portugal

Telegram Android 4.8.11 — 13:24
samsungSM-A520F, Android SDK 26
Redacted IP, Portugal

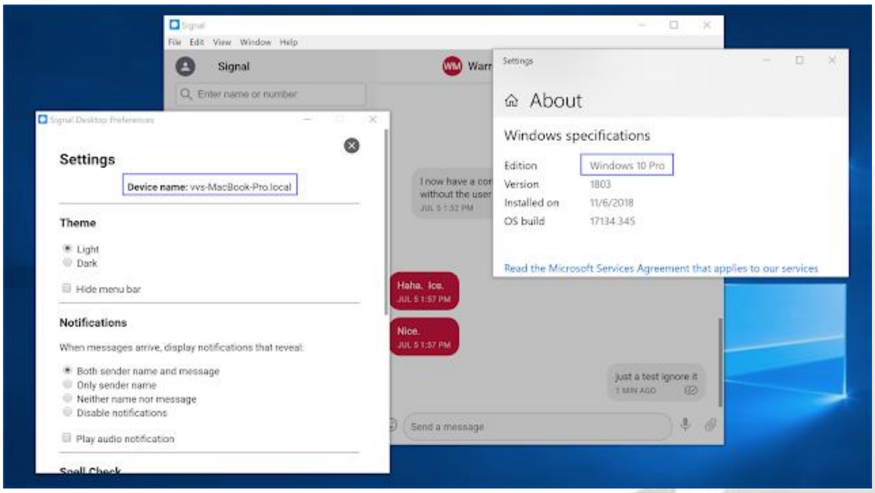
CLOSE

Figure 3. Dual sessions on Telegram desktop environments.

Once the attacker starts the Telegram desktop application using the stolen session information, a new session is established without giving any warning to the user. The user has to check if there is an additional session in use. This is carried out by navigating through the settings, which isn't obvious to the average user. When the message does show up on Telegram, it isn't obvious to the average user, either.

Signal — Desktop session hijacking

Signal handles the session hijacking as a race condition. When the attacker starts the application using the stolen session information, they both compete for the session. As a result, the user will see error messages on the desktop application, but not the mobile device.



Signal Desktop Preferences

Settings

Device name: vvs-MacBook-Pro.local

Theme

● Light
○ Dark

□ Hide menu bar

Notifications

When messages arrive, display notifications that reveal:

● Both sender name and message
○ Only sender name
○ Neither name nor message
○ Disable notifications

□ Play audio notification

Spell Check

Settings

About

Windows specifications

Edition	Windows 10 Pro
Version	1803
Installed on	11/6/2018
OS build	17134.345

Read the Microsoft Services Agreement that applies to our services

I now have a con… without the user… JUL 5 1:52 PM

Haha, Ice. JUL 5 1:57 PM

Nice. JUL 5 1:57 PM

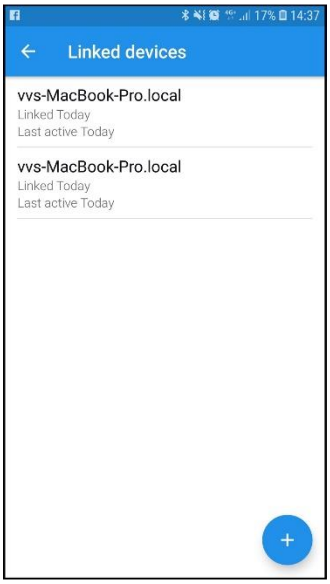
just a test ignore it 1 MIN AGO

Figure 4. Sessions created on Mac will work on Windows and vice-versa.

However, by the time the victim receives these messages, the attacker already has access to all contacts and previous chats which were not deleted.

In order to prevent the race condition, the attacker can simply delete the session information. When the user starts the application, it will receive a request to re-link the application.

For a security expert, this would be a red flag. But for the average user, they may think it's just an error in the application.



Linked devices

vvs-MacBook-Pro.local
Linked Today
Last active Today

vvs-MacBook-Pro.local
Linked Today
Last active Today

Figure 5. Two sessions for the same device.

When the user creates the second session, it will only be visible from the mobile device, and by default, the two sessions will have the same name.

Therefore, the attacker will have the ability to view all messages and even impersonate the victims. The messages sent by the attacker will reach the victim's legitimate devices, but the attacker can delete them while sending them, avoiding detection. If the impersonation is done using the "Disappearing messages" feature, it will be even harder for the victim to identify the imitation.

WhatsApp — Desktop session hijacking

WhatsApp is the only application that has implemented a notification mechanism if there's a second session opened on a desktop. Under normal operations, if an attacker uses the stolen session information, the victim should receive a warning like the image below.

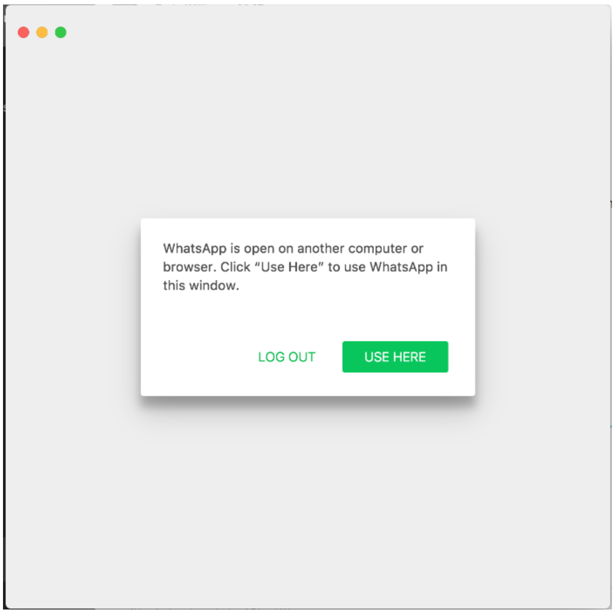
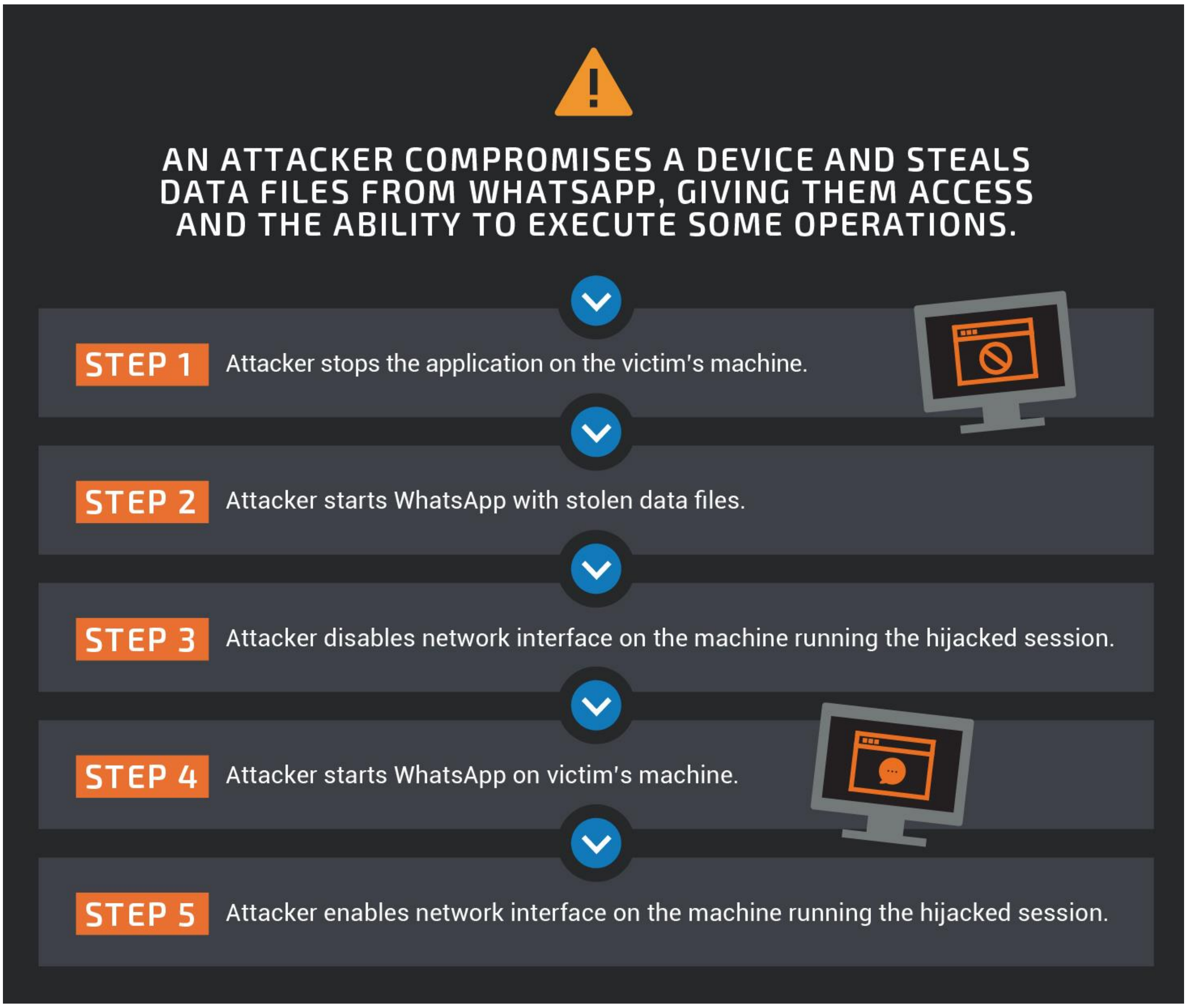

WhatsApp is open on another computer or browser. Click "Use Here" to use WhatsApp in this window.

Figure 6. WhatsApp multiple login notice.

This notice pops up in the application that is online when the second session is created. The second session will be live and usable until the user makes a decision. So, by the time this notice appears, the attacker already has access to all of the victim's contacts and previous messages. The attacker will also be able to impersonate the victims until there is an answer to the message box. In an attack scenario where the victim is away from the terminal, the attacker will have access until the victim is back at the terminal. The victim will have no obvious warning on the mobile device alerting them of what happened. The current notice exists every time the victim uses the desktop client. A second session won't change the warning.

This warning mechanism has a flaw, as it is possible for an attacker to bypass it following the procedure below.

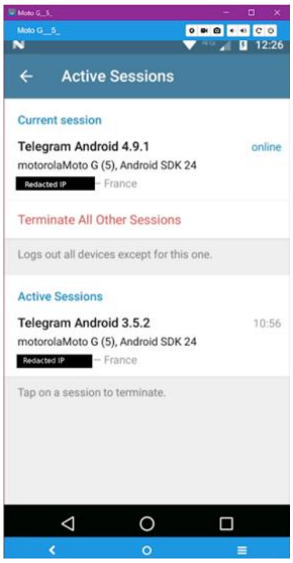

AN ATTACKER COMPROMISES A DEVICE AND STEALS DATA FILES FROM WHATSAPP, GIVING THEM ACCESS AND THE ABILITY TO EXECUTE SOME OPERATIONS.
STEP 1 Attacker stops the application on the victim's machine.
STEP 2 Attacker starts WhatsApp with stolen data files.
STEP 3 Attacker disables network interface on the machine running the hijacked session.
STEP 4 Attacker starts WhatsApp on victim's machine.
STEP 5 Attacker enables network interface on the machine running the hijacked session.

The attacker can simplify the procedure by skipping step 4 and waiting before executing step 5. The result will be the same since they will have access to the same messages. The attacker will only lose access if the victim manually terminates the session on the mobile device.

This vulnerability was disclosed to Facebook according to our coordinated disclosure policy. All the advisory details can be found here.

Telegram — Mobile session shadowing

Session abuse isn't a problem just in the desktop environment. Cloned mobile applications abuse these sessions in the wild.



Active Sessions

Current session

Telegram Android 4.9.1 online
motorolaMoto G (5), Android SDK 24
Redacted IP – France

Terminate All Other Sessions

Logs out all devices except for this one.

Active Sessions

Telegram Android 3.5.2 10:56
motorolaMoto G (5), Android SDK 24
Redacted IP – France

Tap on a session to terminate.

Figure 7. Shadow sessions on a mobile device.

In the mobile environment, users should not be as concerned about their session being compromised, which under normal circumstances, should be much harder to obtain. The fundamental problem lies in the fact that Telegram allows shadow sessions to coexist on the same device based on the same phone number while handling it in different applications.

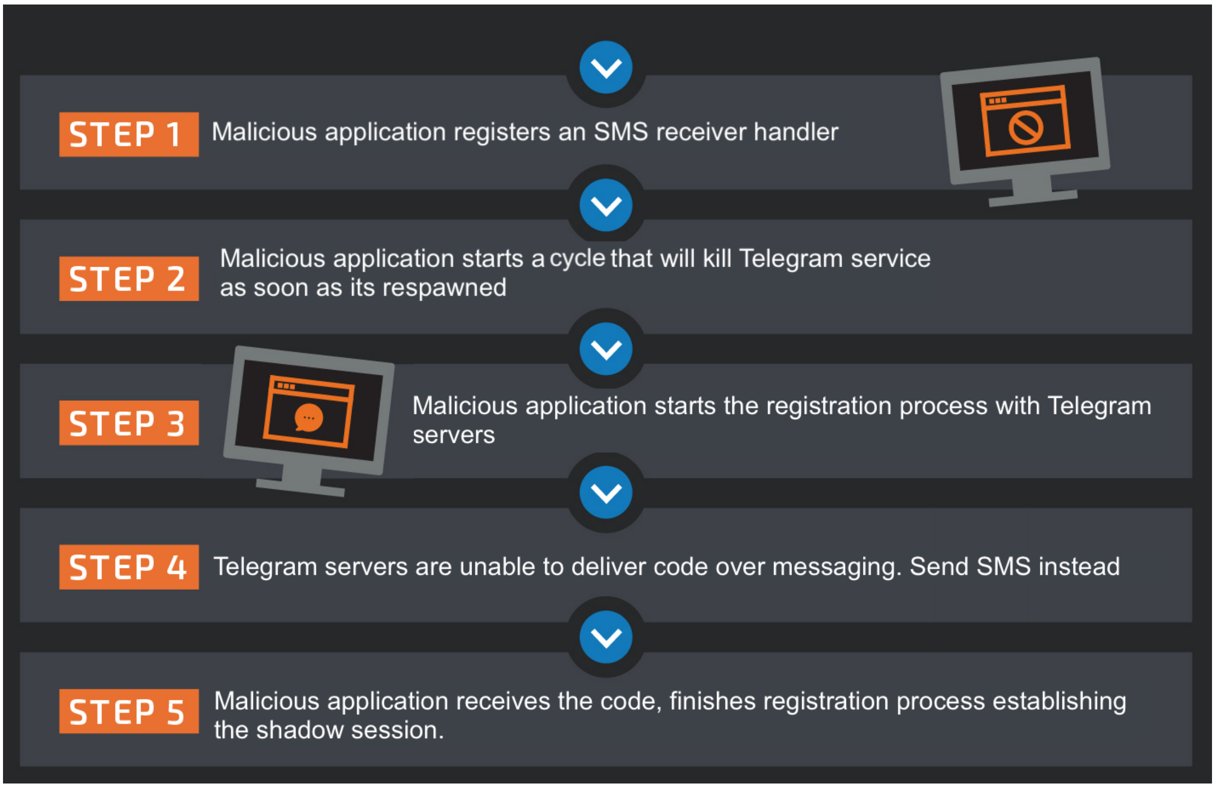
This enables an attack scenario where an attacker can read all messages and contacts on Telegram until the session is terminated. With mobile devices, sessions are never terminated unless the user specifically requests termination through the options menu.

There is another scenario on the Android platform, in which a malicious application could create a shadow session without any user intervention. The malicious application only needs the "read SMS" and the "kill background process" permissions, which are not usually considered as dangerous and could easily pass Google Play store verifications.

The Telegram registration process starts by requesting a phone number, which is confirmed through an SMS that contains a unique code. If a user tries to register the same phone number again, Telegram will send a code over the Telegram channel and not an SMS.

The change in the delivery channel, from SMS to Telegram message, should prevent malicious applications from creating a shadow session without user interaction since they wouldn't be able to read the code. However, if the registration is not completed within a specific time frame, Telegram assumes the user doesn't have access to the Telegram application and will send a new code over SMS.

This backup mechanism creates a race condition that can be exploited by a malicious application, leading to a shadow session being created without user interaction. This entire process is outlined below.



STEP 1 Malicious application registers an SMS receiver handler

STEP 2 Malicious application starts a cycle that will kill Telegram service as soon as its respawned

STEP 3 Malicious application starts the registration process with Telegram servers

STEP 4 Telegram servers are unable to deliver code over messaging. Send SMS instead

STEP 5 Malicious application receives the code, finishes registration process establishing the shadow session.

From this point on, the malicious application will have access to all contacts, past and future messages which are not under the "Secret chats."

Conclusion

Secure instant messaging applications have a solid track record of protecting the information while in transit, even going as far as protecting the information from their own servers. However, they fall short when it comes to protecting application state and user information, delegating this protection to the operating system.

Signal protocol developers predicted this session hijacking. The session management protocol (Sesame protocol) security considerations contains a sub-chapter dedicated to the device compromise, which states, "Security is catastrophically compromised if an attacker learns a device's secret values, such as the identity private key and session state."

This attack vector was even predicted by the protocol developers, as such individual users and corporations should be aware that these applications are not risk free. As such, it becomes more important that companies that use these apps to transmit private and sensitive information employ endpoint technology that better protects these assets.

Source: https://blog.talosintelligence.com/2018/12/secureim.html

3. Hidden Code in Memes Instruct Malware via Twitter

Analysts discover malicious code embedded in tweeted images.

Remember when memes were little more than satirical images overlaid with text? Not anymore. Researchers have identified a new type of malware that receives instructions via hidden code embedded in memes posted to Twitter.

According to researchers, the meme-driven malware is nothing more than a simple remote access trojan (RAT) instructed in a novel way. The first step in the attack is infecting a targeted PC with the RAT – identified as TROJAN.MSIL.BERBOMTHUM.AA. Next, the malware listens for commands from a single Twitter account (created in 2017) and controlled by the malware operator.

“The memes contain an embedded command that is parsed by the malware after it’s downloaded from the malicious Twitter account onto the victim’s machine,” wrote researchers with Trend Micro that discovered the malware and publicly disclosed its findings on Friday.

According to Trend Micro, Twitter disabled the account in question on Dec. 13, 2018. In total, only two malicious tweets were observed by researchers and they were posted to Twitter on Oct. 25 and 26.

The use of Twitter as a means to spread malicious code is nothing new. For nearly a decade, cybercriminals have been using Twitter accounts to spread links containing malicious code and botnet commands.

“This new threat is notable because the malware’s commands are received via a legitimate service (which is also a popular social networking platform), employs the use of benign-looking yet malicious memes, and it cannot be taken down unless the malicious Twitter account is disabled,” wrote researchers.

What’s interesting about this RAT is its use of steganography to send commands to the malware program, and its use of Twitter as a sort of smoke screen to communicate with its malicious servers, undetected.

Researchers said meme images are posted to Twitter where the “malware then parses the content of the malicious Twitter account and begins looking for an image file using the pattern: “<img src=\”(.*?):thumb\” width=\”.*?\” height=\”.*?\”/>” on the account.”

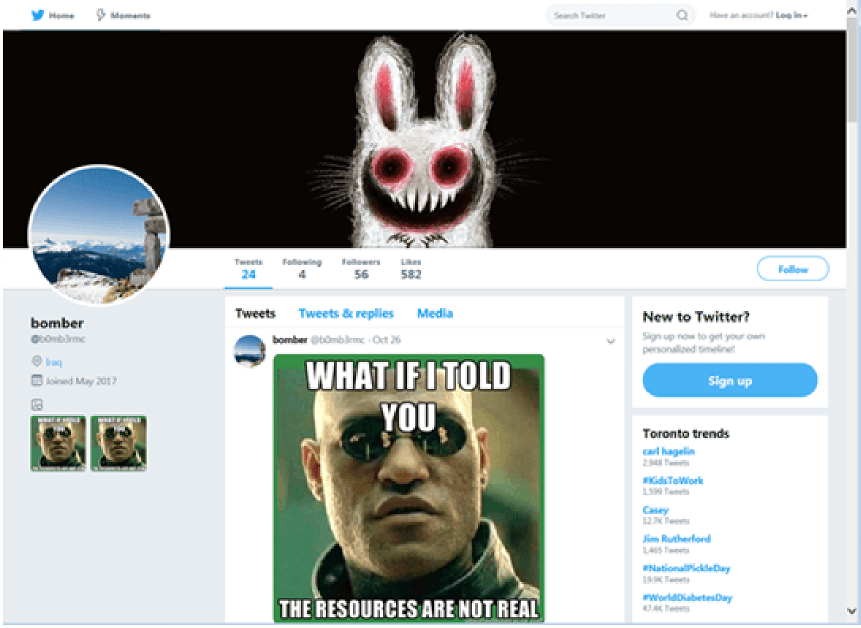


Figure 8. A screen capture of the malicious Twitter account

The code itself contained "/print" commands which instructed the malware to capture screenshots of the affected computer. "The screenshots are sent to a C&C server whose address is obtained through a hard-coded URL on pastebin.com," researchers wrote.

Though only two tweets were found to contain infected memes, the analysts warned that the images included five executable commands, such as "/clip" to see text copied to a user's clipboard, or "/processes" to find out what programs are actively running on the user's computer.

Steganography is a technique that hides code within image files, and is a form of attack not unique to Twitter. For years, cybercriminals have embedded malicious code in image files, often distributed in email malspam campaigns. However, this is the first instance to date that's solely utilized memes, which are viral by nature.

There is evidence researchers were able to nip this attack in the bud, before the memes were able to spread – and the malware along with them. According to an analysis of the malware using VirusTotal the malware first appear in October, around the same time that the target Pastebin post was created.

Still unknown is the identify the hackers including their intentions. However, researchers note there are some indications that this may have been an experiment. The "paste" pointed to a local address, suggesting that the attacker or attackers were merely testing the idea.

Researchers stress that none of the tweets could have caused an infection alone. Instead, they were only a conduit to activate already-infected machines.

Source: https://threatpost.com/hidden-code-in-memes-instruct-malware-via-twitter/140047/

4. Facebook Flaw Exposes Private Photos for 6.8M Users

The bug allowed 1,500 apps built by 876 developers to view users' unposted "draft" photos.

Facebook on Friday disclosed a bug in its platform that it said enabled third-party apps to access unpublished photos of 6.8 million users.

Facebook stores copies of photo drafts, so if someone uploads the photo but doesn't finish posting it, the photo will still be stored in the platform's database. The bug gave third-party apps access to these drafted photos.

The social-media company said that it discovered the glitch in a photo application program interface (API) that plagued the platform for 12 days, between Sept. 13 to Sept 25. The bug, which has since been fixed, gave some third-party apps "access to a broader set of photos than usual," Facebook said.

While Facebook usually only grants apps with permissions access to photos that people share on their timeline, "In this case, the bug potentially gave developers access to other photos, such as those shared on Marketplace or Facebook Stories," Tomer Bar, engineering director at Facebook, said in a post Friday. "The bug also impacted photos that people uploaded to Facebook but chose not to post."

Facebook said that up to 6.8 million users are affected, as well as up to 1,500 apps built by 876 developers. The company said it will alert potentially impacted users.

"Early next week we will be rolling out tools for app developers that will allow them to determine which people using their app might be impacted by this bug," Facebook said. "We will be working with those developers to delete the photos from impacted users."

Facebook has found itself embroiled in an array of security incidents this year – with this one only the latest.

In May, a Facebook software bug switched the "suggested audience" for posts to "public" for 14 millions of users. The glitch meant Facebook users who though they were sharing content with just friends or small groups actually made their posts available to the general public.

In September, Facebook said that hackers had exploited a flaw in its "View As" feature that left the access tokens of almost 50 million Facebook accounts ripe for the taking.

In response to data-related incidents like these and its Cambridge Analytica scandal earlier in March, Facebook has tried to step up its game around security – in March the company announced it would expand its bug bounty program in an attempt to thwart improper data handling third-party app developers.

Source: https://threatpost.com/facebook-photos-exposed/139940/

5. Biometrics: Security Solution or Issue?

Issues still exist when it comes to securing biometrics.

NYC – With more transactions occurring online – and subsequently, the number of data breaches increasing – biometrics are moving to the forefront in discussions as a top way to authenticate data securely.

However, challenges remain. The method is not yet being widely utilized by consumers or enterprises – and for those who are using identification via fingerprint, voice, eye scan or facial recognition, security risks still exist.

Maja Pantic, computing and research director at the Samsung AI Research Center, said at the WSJ Cyber Security Forum in NYC on Tuesday that same emerging models that are making biometrics possible are also being utilized to potentially disrupt the security model behind them.

"These models are powerful tools we can use to generate new data… but also fake data," she said.

The Rise of Biometrics

Ellen Richey, vice chairman and head of risk and public policy at Visa, said that the company, which processes half a billion transactions a day, has seen a marked shift in how consumers buy products.

In today's digitized world, customers have moved to purchasing goods online – meaning that their data are open to widescale breaches. Security experts and credit-card companies have looked to biometrics as a potential solution to this issue.

"Transactions have moved online, where 'something you have' doesn't work – now it's 'something you know,' also known as passwords," Richey said. "Then what happened was the mass proliferation of data breaches. We have to solve for online authentication with something different than 'what you have' and 'what you know,' that is 'what you are' – or biometrics."

Making matters easier, previously companies needed a lot of data to recognize people – but the advent of using machine learning has helped boost facial recognition and other biometrics applications.

Security Challenges Remain

Despite its promise, issues still exist when it comes to biometrics, panelists noted.

One type of technique, dubbed "Deepfake," is an artificial intelligence-based human image synthesis technique. Typically used to create fake pornographic videos or fake news, Deepfake poses a risk to biometrics as it can also potentially be used to create fake profiles, said Pantic.

“People can use this for new voice profiles to trick the system for ID,” said Pantic. “One issue is that when people use the data for generating new data, they base it on this data they already have. That means you can produce profiles very close to existing profiles – and can create profiles.”

At Black Hat 2018, researchers released a slew of PoCs showing how voice authentication can be bypassed. One of these consisted of identifying a target and harvesting about 10 minutes of high-quality audio samples of the victim via public sources such as YouTube, in order to create a fake voice profile.

Making matters worse, Pantic said that the industry is still very far away from technology and knowledge needed to defeat Deepfake techniques.

The Best Biometric Practices

How can companies implement biometrics while still protecting themselves? The answer is to remember that “there is no silver bullet,” said Richey.

For instance, Visa uses various forms of biometrics that take into account behavior such as the way a user holds the mouse or phone; and the platform inspects the data around the transactions themselves. That means looking at whether customers have purchased products at a website before, or where they live (based on opt-in data collection methods).

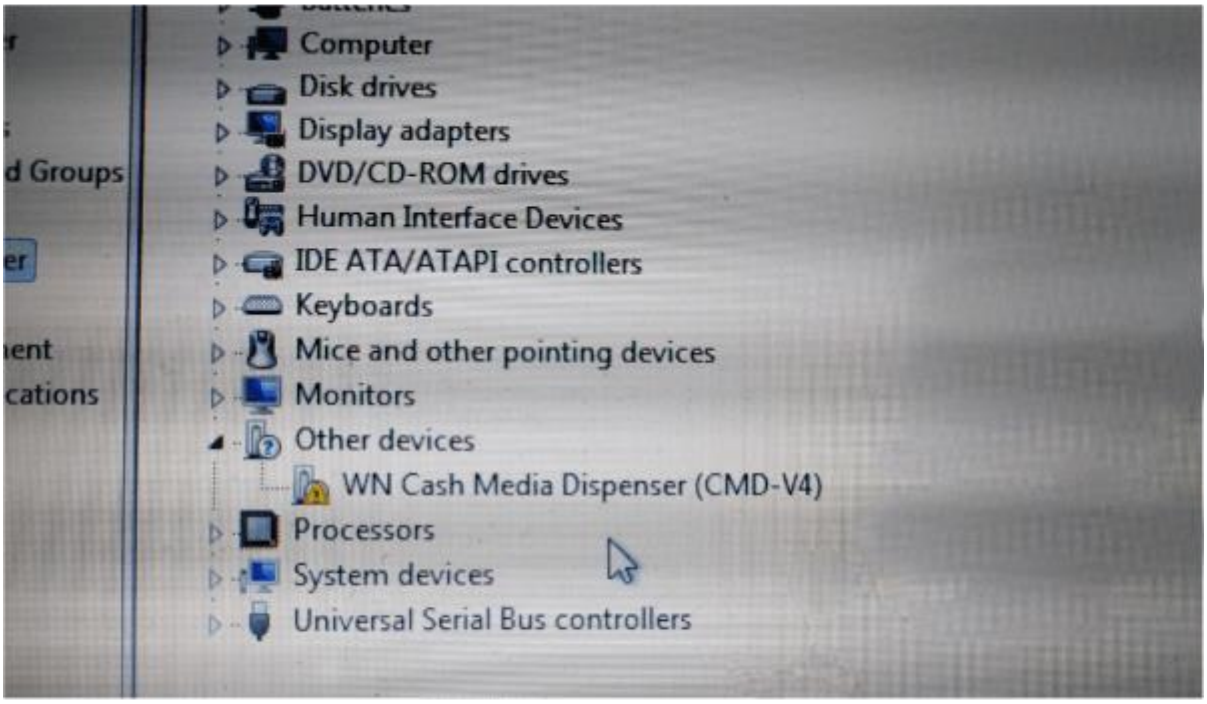
“In our security strategy we never rely on just one thing,” she said. “You can use biometrics, but also use other methods like behavioral characteristics.”

Source: https://threatpost.com/biometrics-security-solution-issue/139781/

6. KoffeyMaker: notebook vs. ATM

Despite CCTV and the risk of being caught by security staff, attacks on ATMs using a direct connection — so-called black box attacks — are still popular with cybercriminals. The main reason is the low “entry requirements” for would-be cyber-robbers: specialized sites offer both the necessary tools and how-to instructions.

Kaspersky Lab’ experts investigated one such toolkit, dubbed KoffeyMaker, in 2017-2018, when a number of Eastern European banks turned to us for assistance after their ATMs were quickly and almost freely raided. It soon became clear that we were dealing with a black box attack — a cybercriminal opened the ATM, connected a laptop to the cash dispenser, closed the ATM, and left the crime scene, leaving the device inside. Further investigation revealed the “crime instrument” to be a laptop with ATM dispenser drivers and a patched KDIAG tool; remote access was provided through a connection to a USB GPRS modem. The operating system was Windows, most likely XP, ME, or 7 for better driver compatibility.



Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Other devices
WN Cash Media Dispenser (CMD-V4)
Processors
System devices
Universal Serial Bus controllers

Figure 9. ATM dispenser connected to a computer without the necessary drivers

The situation then unfolded according to the usual scenario: the cybercriminal returned at the appointed hour and pretended to use the ATM, while an accomplice remotely connected to the hidden laptop, ran the KDIAG tool, and instructed the dispenser to issue banknotes. The attacker took the money and later retrieved the laptop, too. The whole operation could well be done solo, but the scheme whereby a “mule” handles the cash and ATM side, while a second “jackpotter” provides technical support for a share of the loot, is more common. A single ATM can spit out tens of thousands of dollars, and only hardware encryption between an ATM PC and its dispenser can prevent an attack from occurring.

Overall, the attack was reminiscent of Cutlet Maker, which we described last year, except for the software tools. We were able to reproduce all the steps of KoffeyMaker in our test lab. All the required software was found without too much difficulty. Legitimate tools were used to carry out the attack with the exception of the patched KDIAG utility, which Kaspersky Lab products detect as RiskTool.Win32.DIAGK.a. Note that the same version of this program was previously used by cybercriminals from the Carbanak group.

Source: https://securelist.com/koffeymaker-notebook-vs-atm/89161/

7. Netbooks, RPis, & Bash Bunny Gear – Attacking Banks from the Inside

Multiple banks in Eastern Europe have been attacked from inside their network via various electronic devices connected directly to the company's own infrastructure, security researchers have discovered.

Where possible, the adversary made an effort to hide the entry point by planting the malicious devices in a way that did not attract attention. The losses created this way are estimated to tens of millions of dollars.

Direct access to the local network

Dubbed DarkVishnya, the attacks targeted at least eight banks using readily-available gear such as netbooks or inexpensive laptops, Raspberry Pi mini-computers, or a Bash Bunny - a USB-sized piece hardware for penetration testing purposes that can pose as a keyboard, flash storage, network adapter, or as any serial device.

They gained access to the local network from various places inside the victim's central or regional offices, and even from company branches in a different country.

Given their position, the devices could launch attacks that bypassed network defenses and could easily run reconnaissance routines, which are the first step of a cyber attack once on the target infrastructure.

Sergey Golovanov from Kaspersky Lab says that the researchers discovered this attack method between 2017 and 2018 while investigating cybertheft incidents.

"Inside the local network, the device appeared as an unknown computer, an external flash drive, or even a keyboard," he details.

To control the rogue gear remotely, the attackers used a built-in or USB-powered GPRS/3G/LTE wireless modules.

In the second stage of the attack, the intruders scanned the digital premises in search of open resources such as shared folders and web servers with public access.

The goal was to identify and collect valuable information like login credentials for systems used for making payments. To this end, the threat actor tried to brute-force their way in or intercept traffic to extract login data.

Evading firewall restrictions was possible through reverse TCP shells and the use of a different payload to create the communication tunnel. If a ll went well, the adversary would log into the target system and gain persistence.

Golovanov says that the threat actor launched on the compromised system malicious services created with the MSFvenom tool from the Metasploit Framework.

Fileless attacks are difficult to spot

The success of these operations is owed to the fact that they did not rely on specific malware to achieve their goals but relied on tools like PowerShell that could bypass whitelisting technologies and domain policies in most cases.

Although widely abused by cybercriminals to run malicious scripts, PowerShell is a legitimate component that is typically available on target machines.

Some system administrators block PowerShell on network machines to minimize the attack surface. If this was the case, the DarkVishnya attacks would use the Impacket Python library, winexesvc.exe or psexec.exe for remote execution of processes.

All three are legitimate tools used by admin to run commands on remote machines and redirect the output on the local system. PsExec has been used maliciously since at least 2004 and it was used by NotPetya ransomware for lateral movement.

Crims take a page from pentesters' book

This method of compromise is not new. It has been used in attacks against banks as early as 2013, when a gang stole over £1.3 million from Barclays Bank by connecting a keyboard video mouse (KVM) switch with a 3G router to a computer in the bank.

Penetration testers also use this method to breach defenses of a target with strong protections against outside access. Bash Bunny, for example, is specially built for this purpose as its form factor resembles a flash drive and once connected to a computer it can run scripts that give access to assets on the network.

Source: https://www.bleepingcomputer.com/news/security/netbooks-rpis-and-bash-bunny-gear-attacking-banks-from-the-inside/

8. The Ransomware Doctor Without A Cure

When individuals and organizations alike rely so much on their computers to get work done, there is nothing they hate more than being held hostage by ransomware and often hold a deep resistance to paying the demanded ransom. After all, when there is no guarantee the criminal will keep his word and release the files, why pay up? To avoid paying then, victims can hire an IT consultancy to help them unlock their files.

However, Check Point Research recently discovered a new development in the ransomware industry of an IT consultancy, in this case a Russian company named 'Dr. Shifro', that claims to legitimately unlock encrypted files but in fact merely pays the ransomware's creator themselves and passes on the cost to the victim – at a massive profit margin.

Ransomware By the Numbers

In 2017, ransomware took center stage with the catastrophic attacks of WannaCry, NotPetya and Bad Rabbit, and it has continued to be a major menace this year too. From the crippling effect it had on the City of Atlanta earlier this year, preventing vital services within the city from functioning, to the constant havoc caused on the healthcare sector. Indeed, the healthcare industry is one which continues to bear the brunt of ransomware attacks with some ransom demands reaching as high as $2.8 million in some cases. Such demands are considered rare, however, with the average demand around $10,000.

According to Europol's 2018 Internet Organized Crime Threat Assessment, the ransomware industry is now worth an estimated $5 billion that is drained yearly from the global economy. In fact, it is very much a staple attack tool for cyber criminals everywhere and has also allowed for subsidiary cottage industries to spring up around it. These include ransomware-as-a-service (RaaS) offerings that allow those with very low technical know-how to get in on the act by spreading the ransomware built by those more proficient. In addition, ransomware affiliate programs have grown to allow the ransomware creators to claim a cut from their affiliates who spread this malware.

As we will now see, though, the discovery of Dr. Shifro is the latest development of the ever growing and changing ransomware landscape.

Who You Gonna Call?

When access to much needed files are locked and held to ransom at such high prices, it's no wonder that organizations will do almost anything to restore their access to them.

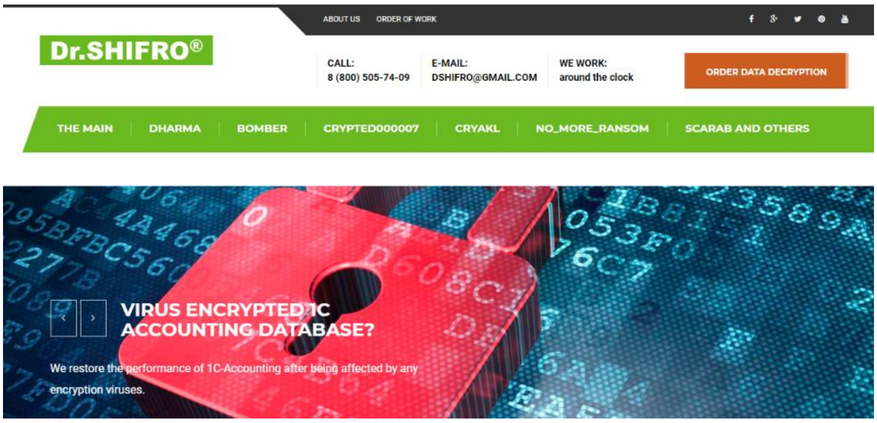
At this point there are three possible options available:

- Restore any locked files from backup.
- Pay the ransom to the threat actor responsible for locking those files in the first place.
- Pay an IT consultant who may be able to unlock the files without paying the ransom.

For those with no file back-up plan in place or who do not want to pay the ransom amount, the third option is usually a sensible choice. Unfortunately, though, it is here that Check Point Research discovered a unique and worrying new development in the ransomware landscape.

Something first seemed off when our team came across a certain 'IT consultancy', promoted online as 'Dr. Shifro', that offered only one service – helping ransomware victims unlock their files. For an IT consultancy to offer only one unique service is highly unusual and arguably suspicious.

In addition, Dr. Shifro promises to perform dazzling feats of cyber wizardry to unlock files held captive by the Dharma/Crisis ransomware (for which no decryption key is available), among others. So, whereas IT services such as these usually explain they can only try and do their best, with no promises made, it seemed strange that Dr. Shifro guarantees to unlock files for ransomware that has no public key even available. Now that's quite a promise!



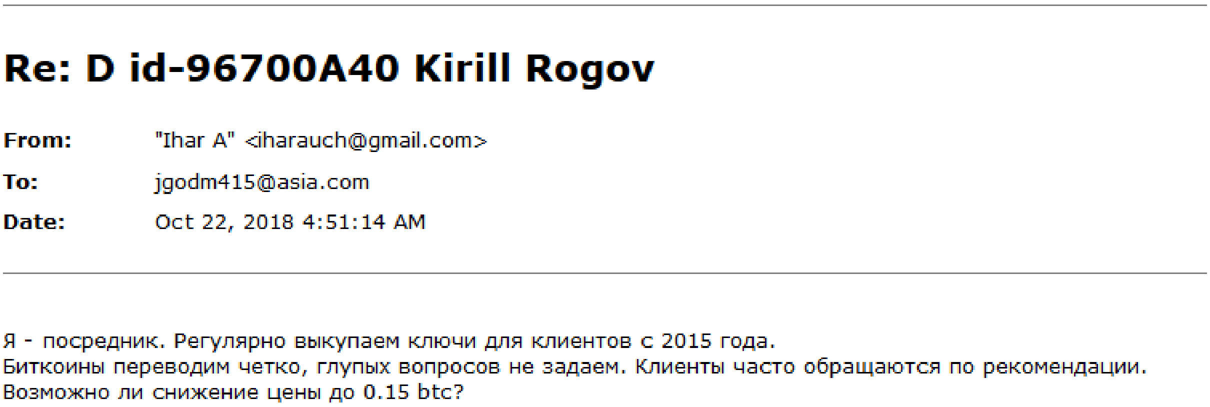
VIRUS ENCRYPTED 1C ACCOUNTING DATABASE?

We restore the performance of 1C-Accounting after being affected by any encryption viruses.

Figure 10. Dr.Shifro's website advertising his ransomware decryption services.

After some undercover investigation, it soon appeared that Dr. Shifro was actually making contact with the ransomware's creator themselves and making a deal with them to unlock the victim's files in return for the ransom payment ($1300). Dr. Shifro would then pass that cost on to the victim with his own fee charged on top (another $1000).

Below is part of the correspondence between Dr. Shifro and a ransomware creator where we can get a glimpse of how Dr. Shifro's 'consultancy' works. By connecting directly with the threat actor to collect the decryption key, in return for payment, Dr. Shifro simply acts as a broker between victim and attacker.



Re: D id-96700A40 Kirill Rogov

From:	"Ihar A" <iharauch@gmail.com>
To:	jgodm415@asia.com
Date:	Oct 22, 2018 4:51:14 AM

Я - посредник. Регулярно выкупаем ключи для клиентов с 2015 года.
Биткоины переводим четко, глупых вопросов не задаем. Клиенты часто обращаются по рекомендации.
Возможно ли снижение цены до 0.15 btc?

Figure 11. Part of the correspondence between Dr. Shifro and the Ransomware creator.

Translation of Dr.Shifro's email to ransomware creator: I'm an intermediary. We redeem keys for clients since 2015 on a regular basis. Send bitcoins tight, don't ask dumb questions. Clients frequently addressed under recommendation. Could you give a discount to 0.15 btc?

This creates an attractive business model. After all, it would seem that all parties win. The victim has their files decrypted, the cyber criminal gets his ransom payment and Dr. Shifro, at an almost 100% markup, earns a handsome 'broker' fee.

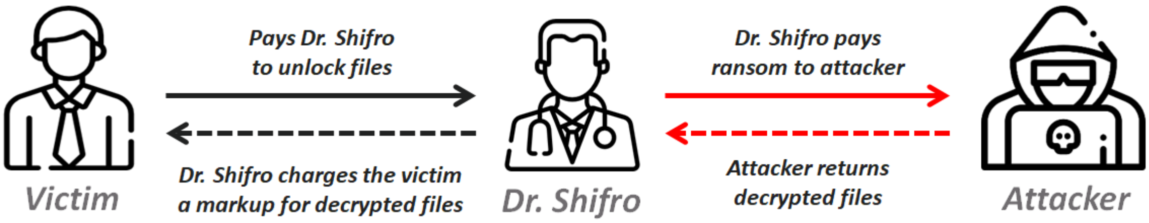

Victim
Pays Dr. Shifro to unlock files
Dr. Shifro charges the victim a markup for decrypted files
Dr. Shifro
Dr. Shifro pays ransom to attacker
Attacker returns decrypted files
Attacker

Figure 12. Dr.Shifro's business model

Key Takeaways

The first thing to bear in mind when coming across services like Dr. Shifro is "if it sounds too good to be true, it probably is." Whereas there are legitimate IT consultancies that can help you recover your systems and files from a ransomware attack, they will usually not make promises they cannot keep. In fact, they will only be as confident in what they can offer as the decryption keys that are already publicly available online and merely perform these decryption services for those who may be unable to do so themselves. Anyone claiming otherwise should be approached with caution.

With ransomware being such a devastating and profitable form of attack, we are certain to see the evolution of both the malware itself and the ecosystem it operates within continue. As well as the Ransomware-as-a-Service and ransomware affiliate industry that has sprung up in recent years, the creativity of cyber criminals clearly seems to still have much steam. Indeed, the business model that Dr. Shifro has created is an attractive one that could easily be replicated by other entrepreneurial scam artists and thus serves as a new development of the ransomware industry that both individuals and organizations should be wary of.

Of course, organizations are well advised to be using anti-ransomware prevention solutions across their network in order to avoid being infected in the first place. For this reason we recommend solutions that do not rely on signatures only to identify the various ransomware strains and is able to emulate and extract suspicious files in a virtual sandbox and automatically recover encrypted files.

If you have been affected by ransomware, please visit Europol's 'NoMoreRansom' site for further advice and ways to unlock encrypted files.

For full technical details on how this undercover investigation was carried out, please visit Check Point Research.

For more information about how you can protect your organization from ransomware, please read about Check Point's Anti-Ransomware solution.

Source: https://blog.checkpoint.com/2018/12/10/ransomware-shifro-scam-russia-cyber-crime/

9. Logitech Keystroke Injection Flaw Went Unaddressed for Months

The flaw allows a remote attacker to gain full access over a machine.

Computer peripheral giant Logitech has finally issued a patched version of its Logitech Options desktop app, after being taken to task for a months-old security flaw. The bug could have allowed adversaries to launch keystroke injection attacks against Logitech keyboard owners that used the app.

Google Project Zero security researcher Tavis Ormandy found the bug in September and publicly disclosed the vulnerability this week. The Logitech Options app lets users customize the functions of their Logitech computer peripherals, including mice, keyboards and touchpads.

Logitech Keyboard Vulnerability Ormandy reported the flaw stems from the fact that the app opens up a WebSocket server that allows outside access to the app from any website, with minimal authentication.

"The only 'authentication' is that you have to provide a [process ID] of a process owned by your user, but you get unlimited guesses so you can bruteforce it in microseconds," he explained in a Project Zero bug report that went live this week.

From there, a malicious actor could use a rogue website to send a range of commands to the Options app and change a user's settings. In addition, a malicious actor could send arbitrary keystrokes by changing some simple configuration settings. That in turn would allow a hacker to access all manner of information and even take over a targeted machine.

Further, the app is set to auto-run upon boot-up, so users of the desktop app are essentially running Options persistently in the background – giving any attacker near-continuous access as long as the user's machine is switched on.

Ormandy decided to publicly disclose the bug on Wednesday after Logitech didn't address the flaw for three months, despite assurances to the researcher that it would.

"Had a meeting with Logitech engineers on the 18th September, they assured me they understood the issues and were planning to add Origin checks and type checking," he said. "There was a new release on October 1st, but as far as I can tell they did not resolve any of the issues. This is now past deadline, so making public."

Patched Version Made Available

The bug report got some attention on Twitter, with others chiming in that the same problems exist in the Mac version. Late Thursday the new version was pushed out:

> Hi, the release of Logitech Options 7.00, which addresses Origin checks and type checking, is now live and can be downloaded for Windows and Mac.
>
> — Logitech (@Logitech) December 13, 2018

Release Options 7.00.564 addresses the vulnerability, Logitech said, but as of Friday morning Ormandy sounded skeptical.

“On the Logitech webpage they mention as changes for 7.00.564: ‘You can now backup your device settings to the cloud automatically after creating an account. Log into your Options account and download the backed up settings to set up your device easily on any computer. Bug fixes and improvements.’ (Which can mean anything…)” Ormandy wrote.

Source: https://threatpost.com/logitech-keystroke-injection-flaw/139928/

10. Remote Firmware Attack Renders Servers Unbootable

Security researchers have found a way to corrupt the firmware of a critical component usually found in servers to turn the systems into an unbootable hardware assembly. The recovery procedure requires physical intervention to replace the malicious firmware.

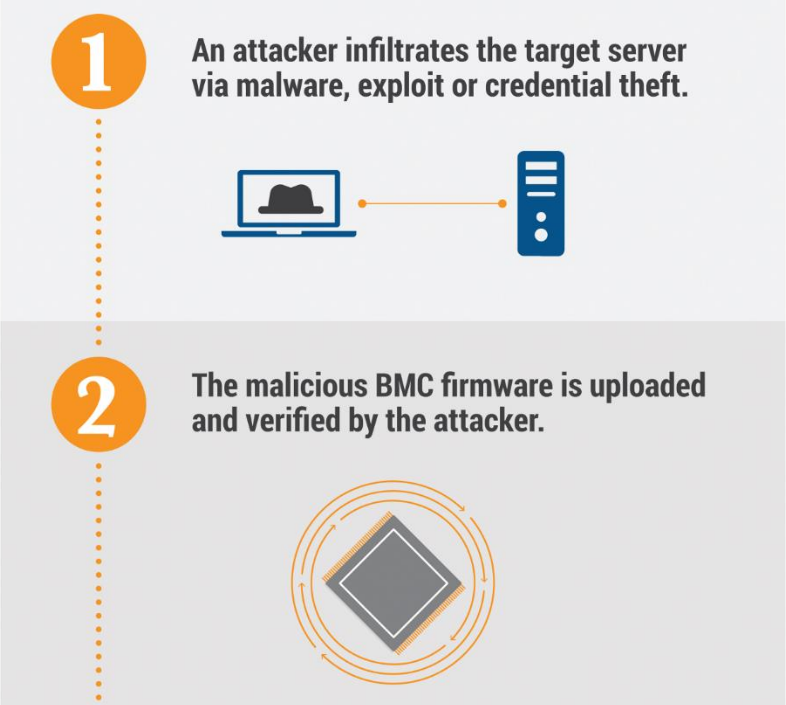
Achieving this is done via regular tools used to keep the baseboard management controller (BMC) up to date.

BMCs are specialized microcontrollers (more like independent micro-computers) embedded on virtually all server motherboards; they are also present in high-end switches, JBOD (just a bunch of disks) and JBOF (just a bunch of flash) types of storage systems.

Apart from getting information about the system health, administrators can use BMCs for remote management of the unit. They can configure the server as well as reinstall the operating system and update the host system firmware.

Next level in destructive cyber attacks

Although deploying the malicious BMC update is possible from a remote location, the destructive step represents the final stage of an attack, so initial access to the target is needed.



1 An attacker infiltrates the target server via malware, exploit or credential theft.

2 The malicious BMC firmware is uploaded and verified by the attacker.

Using the host-based interface known as the Keyboard Controller Style (KCS), researchers from firmware and hardware security firm Eclypsium were able to pass a malicious firmware image to the computer's BMC.

It is worth noting that KCS is part of the Intelligent Platform Management Interface (IPMI) specification, where serious security risks have been found before. The US-CERT in 2013 issued an alert on the risks of IPMI, and guides for penetration testers are easily available.

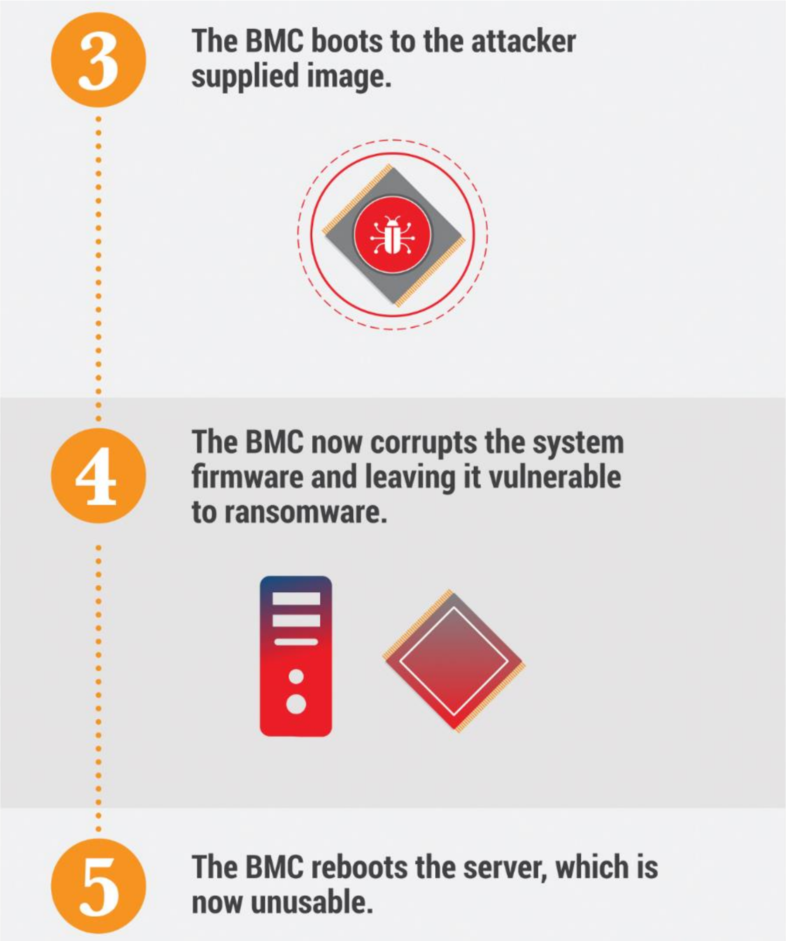
Eclypsium researchers say that authentication or credentials are not necessary to update the BMC firmware with a custom version. In a video published today, they show the steps for updating the BMC with a malicious firmware, rendering the server unusable.

https://www.youtube.com/watch?v=cAfTgma5CsM

"This malicious BMC firmware update contains additional code that, once triggered, will erase the UEFI system firmware and critical components of the BMC firmware itself," they explain in a blog post today.

The modifications made tot he host and the BMC prevent system recovery actions since booting is no longer an option.

For security reasons, BMCs are protected through network isolation, but this precaution is no good if the host is directly targeted. Such an attack can follow the beaten path of a cyber attack that starts with the initial reconnaissance stage and then develops persistence. A more advanced adversary could also poison the supply chain to skip the initial steps of the compromise.



3 The BMC boots to the attacker supplied image.

4 The BMC now corrupts the system firmware and leaving it vulnerable to ransomware.

5 The BMC reboots the server, which is now unusable.

Eclypsium says that an attack of this type "could also be easily scheduled to execute at a specific time. They can be implemented as a kill-switch feature in the malicious software, firmware, or hardware components."

Bringing the server back online

Victims of firmware-level attacks have few options to recover and by the time everything is up and running the losses incurred could have a permanent impact on the future of the business.

Replacing the corrupt firmware requires special tools and knowledge. Each server whose BMC has been corrupted has to be opened to physically connect to the chip and update the firmware with a good version.

This is a highly technical, slow operation performed by specialized services that are not cheap. By the time the systems are up and running, the financial losses could be enormous.

For instance, following the NotPetya attack last year, Maersk container shipping company had to reinstall over 4,000 servers, 45,000 PCs, and 2500 applications.

Although the company was just a collateral victim, they estimate losses to be between $250 and $300 million.

Recovery from data-wiping attacks is quicker

Destructive attacks meant to disrupt the target's activity are not new and have been happening since at least 2012, the most recent incident of this kind occurring this month, via Shamoon.

Malware like NotPetya, Shamoon, Destover, and StoneDrill show a clear interest in causing damages by wiping data on the victim hosts.

However, if proper backup policies and infrastructure are in place, victims can recover from these attacks and minimize financial loss.

Eclypsium's demo shows that firmware-level attacks can be much more damaging and do not require physical access. Data centers and cloud applications are potential targets; taking them offline, even for a short period, could have a significant impact on a business.

Source: https://www.bleepingcomputer.com/news/security/remote-firmware-attack-renders-servers-unbootable/

11. 123456 Is the Most Used Password for the 5th Year in a Row

For the 5th year in a row, "123456" is most used password, with "password" coming in at second place. Even in the wake of a constant stream of data breaches, hacks, and ransomware attack reports people continue to utilize weak passwords that not only put their information at jeopardy, but also their organization's data.

In SplashData's 8th annual worst passwords list, the password management company analyzed more than 5 million leaked passwords to come up with their list of most used passwords. According to their report, the top 10 most used passwords are:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

"Bad habits die hard, according to SplashData's eighth annual list of Worst Passwords of the Year," stated SplashData's press release. "After evaluating more than 5 million passwords leaked on the Internet, the company found that computer users continue using the same predictable, easily guessable passwords. Using these passwords will put anyone at substantial risk of being hacked and having their identities stolen."

Password management company Dashlane also released a report this week that focuses on the biggest password mistakes of the year. Topping the list is Kanye West, who in full view of television cameras entered the password "000000" into his cell phone to unlock it.

The full list of Dashlane's "Worst Password Offenders" is listed below.

1. **Kanye West**: West tops the list of offenders by entering in a password of "000000" to unlock his mobile phone while meeting with President Trump in a room full of television cameras.
2. **The Pentagon**: In a Government Accountability Office (GAO) report, it was found that "credentials management being so poor that one team was able to guess the admin password of a system in nine seconds. The most likely reason for this was that the administrators did not change the default passwords in the software installed on the weapon system."
3. **Cryptocurrency owners**: As the value of cryptocurrencies boomed, users discovered that they no longer remembered the passwords to access their wallets. Some owners who wanted to sell went as far as hiring hypnotists to help remember their passwords.
4. **Nutella**: Nutella gave out the posted a bizarre tweet telling advising their followers to use "Nutella" as their password. Nuff said on this one.
5. **U.K. Law Firms**: Over one million corporate email and password combinations from 500 of the UK's top law firms were discovered on the dark web.
6. **Texas**: Texas left the voter records of over 14 million residents exposed on a server without a password.
7. **White House Staff**: A DC staffer wrote his email login and password on official White House stationary and then left it at a Washington, D.C. bus stop. Oops.
8. **Google**: An engineering student from India was able to access a TV broadcast satellite after logging into Google admin pages using a blank username and password.
9. **United Nations**: U.N. staff were using Trello, Jira, and Google Docs to collaborate on projects, but forgot to secure them with a password! This allowed anyone to access the docs that contained confidential information, communications, and plaintext passwords.
10. **University of Cambridge**: The university added a plaintext password to a GitHub project that allowed anyone to access the data of millions of Facebook users being studied by the university's researchers.

As always, users should create strong and unique passwords at every site they visit. These passwords should contain at least 8 characters, upper and lower case letters, numbers, and symbols such as %$#!. To aid them in remember unique passwords at each site, they can use a password management utility to store the passwords.

Source: https://www.bleepingcomputer.com/news/security/123456-is-the-most-used-password-for-the-5th-year-in-a-row/

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

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.