



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

Monthly Security Bulletin

September 2019

This security bulletin is powered by

Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.



Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state of the art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Contents

Executive summary.....	5
1. CafePress Data Breach Exposes Personal Info of 23 Million Users.....	7
2. Leveraging AI to Win the Cybercrime Arms Race.....	9
The Digital Transformation Challenge For Business.....	9
The Digital Transformation Opportunity For Cybercriminals.....	9
AI Takes Everything To The Next Level	10
Fighting Fire With Fire	10
1. 'Coordinated Ransomware Attack' in Texas Hits 23 Local Governments.....	11
23 may not be the final count	11
Ransomware is big in U.S.....	12
2. \$11M Email Scam at Caterpillar Sales Office Pinned to Nigerian Man.....	13
Long time BEC scammer.....	13
Tricks of the trade.....	14
Wrapping things up.....	14
3. What Makes Local Government an Enticing Cyber Target?.....	15
Attractive Data.....	15
Growing Cybersecurity Challenges	15
Breaking Down Silos.....	16
Budget Constraints.....	16
Ransomware is Top of Mind.....	16
What's Needed: Simpler Security Solutions	16
4. KuppingerCole Report on IT Landscape's Complexity	17
Defining Data Protection in an Age of IT Complexity	17
A Leader in Database and Big Data Security.....	18
5. How to Prepare for Misconfigurations Clouding the Corporate Skies	19
Setting Up the Cloud.....	20
Securing the Cloud from Stormy Weather.....	20
Finding the Data Leak in the Cloud	21
6. Visa Adds New Threat Detection to Prevent Payment Fraud	21
New fraud detection capabilities	22
7. PokerTracker.com Hacked to Inject Payment Card Stealing Script	23
Magecart loading in poker app	23
Outdated CMS.....	24
8. Agent 1433: remote attack on Microsoft SQL Server.....	24
Attack description.....	25
Examples of jobs.....	25
MD5.....	27
9. Asruex Backdoor Variant Infects Word and PDFs Through Old Vulnerabilities ..	27

Technical details.....	27
Infected PDF files.....	28
Infected Word documents.....	30
Infected executables.....	31
Conclusion and security recommendations	31
Indicators of Compromise (IoCs).....	32
10. Unpatched Squid Servers Exposed to DoS, Code Execution Attacks	33
Some unpatched servers exposed to attacks	33
11. ThreatList: Half of All Social Media Logins Are Fraud.....	35
Bots vs. Humans.....	36
Attacks by Industry.....	36
12. Hostinger Data Breach: 14M Customer Passwords, Personal Data at Risk	37
13. Malware Operation Making Millions Defeated by Design Flaw	38
Botnet handler(s) may have made millions.....	39
Author leaves obvious traces.....	39
Most victims in Latin America.....	40
Design flaw brings botnet down	40

Executive summary

1. CafePress, a well-known custom T-Shirt and merchandise site, suffered a data breach that exposed the personal information of 23 million of their customers as per notifications from Troy Hunt's Have I Been Pwned service. The site was hacked in February 2019 and the breach contained Email addresses, Names, Passwords hashed with weak algorithm, Phone numbers, and Physical addresses [→](#)
2. With AI used by both cyber attackers and cyber-defenders, a report written by Fortinet's Global Security Strategist, Derek Manky outlines ways how it will change the field [→](#)
3. Following ransomware payouts by two cities in Florida, now Texas is currently fighting an unprecedented wave of coordinated ransomware attacks that has targeted local government entities in the state, with at least 23 impacted by the attacks. Attackers are trying to extort more than 2.5 mln USD [→](#)
4. A Nigerian national that was on Forbes' list of the most promising entrepreneurs in Africa is accused of business email compromise fraud that stole \$11 million from one US corporate victim alone. His account was also linked to other criminal activity [→](#)
5. Local government IT departments face pressures from all sides: citizens are demanding digital services and frictionless online experiences, government leaders want to reduce risk within the IT infrastructure, and also face increasingly stringent data security compliance requirements all within limited budgets. But what makes the local government a cyber target? [→](#)
6. New report from KuppingerCole recognizes the shift that has occurred in the market over the last two years: "A notable change in the direction the market is evolving has become apparent: as the amount and variety of digital information an organization is managing grows, the complexity of the IT infrastructure needed to support this digital transformation grows as well." [→](#)
7. With 65 percent of organizations using some form of an infrastructure-as-a-service (IaaS) model and a 27.7 percent increase in cloud-related security incidents from the last year according to report from McAfee, what organizations can do to prepare and protect their data from misconfigurations in the cloud ? [→](#)
8. Visa announced the addition of new fraud threat detection and blocking technologies to their VTI platform, designed to boost transaction security and, implicitly, the integrity of its payments ecosystem. The technologies include deep learning to analyze card-

not-present transactions on Visa's database, testing environment to examine client processing, business logic and configuration and real-time scanner of eCommerce sites to detect skimmer malware [→](#)

9. Poker Tracker website, that distributes popular software, used by poker enthusiasts to improve their winning chances had been compromised and loaded malicious MageCart JavaScript that stole payment information from customers. [→](#)
10. Companies all over the world use Microsoft SQL Server for database management. Highly popular yet usually insufficiently protected, this DBMS is a target of choice for hacking. One of the most common attacks on Microsoft SQL Server — the remote attack based on malicious jobs — has been around for a long time, but it is still used to get access to workstations through less-than-strong administrator password and is especially popular among Asian attackers [→](#)
11. Since it first emerged in 2015, Asruex malware has been known for its backdoor capabilities and connection to the spyware DarkHotel. However, new variant is identified that can also act as an infector particularly through the use of old vulnerabilities, which inject code in Word and PDF files respectively. [→](#)
12. Multiple versions of the Squid web proxy cache server built with Basic Authentication features are currently vulnerable to code execution and denial-of-service (DoS) attacks triggered by the exploitation of a heap buffer overflow security flaw. The flaw was patched by the web proxy's development team with the release of Squid 4.8 on July 9. [→](#)
13. More than half of logins (53 percent) on social media sites are fraudulent; and 25 percent of all new account applications on social media are fake, according to a recent analysis in Arkose Labs Q3 Fraud and Abuse Report that analyzed more than 1.2 billion transactions [→](#)
14. Hostinger, a popular web, cloud and virtual private server hosting provider and domain registrar with 29 million+ users, has notified its customers that a breach of one of its servers potentially gave bad actors access to the hashed passwords and personal non-financial data of more than 14 million customers. As result company has reset all passwords [→](#)
15. Retadup botnet that has infected more than 850,000 systems has been brought down thanks to a design flaw in the communications protocol, uncovered by Avast working with the French National Gendarmerie. The botnet was mostly used for cryptojacking and first was identified in 2017 in hospitals in Israel. Recently most Retadup victims were in Spanish-speaking countries, with Peru leading the pack with over 320,000 infections. [→](#)

1. CafePress Data Breach Exposes Personal Info of 23 Million Users

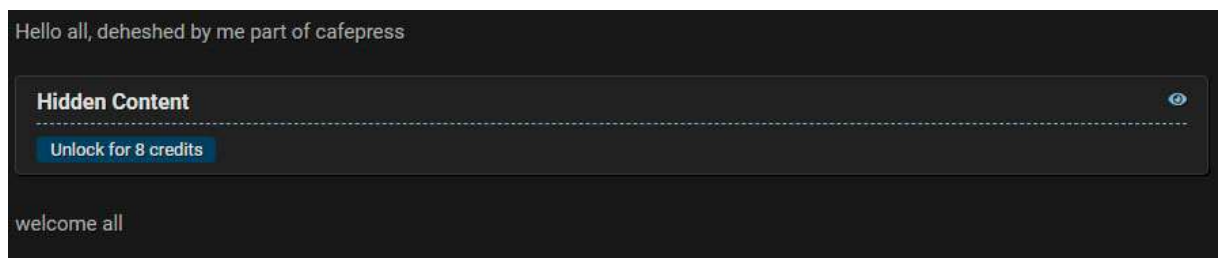
CafePress, a well-known custom T-Shirt and merchandise site, suffered a data breach that exposed the personal information of 23 million of their customers.

Users became aware of the breach today, not through CafePress, but through notifications from Troy Hunt's Have I Been Pwned service.

After hearing about a CafePress data breach being circulated, Hunt solicited the help of security researcher Jim Scott who had helped him with other data breaches in the past, such as Evite.

"Security researcher Jim Scott is just fine. About 2 weeks ago I got notified by Troy that CafePress.com data breach was circulating and if I had seen it. At that time, the only public source of this data breach was from the data breach search engine WeLeakInfo and was not being sold as far as I know. With the help of my colleagues, I started to search for the database more thoroughly until I found it," Scott told BleepingComputer via email.

Research by BleepingComputer shows that a dehashed CafePress database of approximately 493,000 accounts was being sold on hacker forums. It is not known if this is related to the same breach.



According to HIBP, CafePress was hacked in February 2019 and exposed the personal information for 23,205,290 users. This exposed data includes Email addresses, Names, Passwords, Phone numbers, and Physical addresses.

Scott further told BleepingComputer that half of the compromised user's passwords were encoded in base64 SHA1, which is a very weak algorithm by today's standards. The other half of the users contained third-party tokens for logins through Facebook and Amazon.

"It came to my attention that Troy forgot to add that passwords were also affected in this security incident when first announcing this data breach, which has now been corrected. Out of the 23 million compromised users, roughly half of them had their passwords exposed encoded in base64 SHA1, which is a very weak encryption method to use especially in 2019 when better alternatives are available. The remaining users who used CafePress through third-party applications, such as FaceBook or Amazon, had no compromised passwords."

At the time of this writing, CafePress has not responded to BleepingComputer's queries and has not issued a statement regarding the data breach.

The only indication that something is wrong is that CafePress users are being forced to reset their password when they try to login to the site. In this password reset policy there is no mention of the breach as well.

Attention:


We've updated our password policy and are requiring all users to change their passwords.


Please click the [forgot password](#) link below.

Passwords must meet the following conditions:

- have a minimum of 8 characters and a maximum of 128 characters
- include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~ "

If you still experience problems please contact customer service at support@cafepress.com for further assistance.





OR

Sign in with your CafePress Account

Email Address

Password

Stay signed in[Forgot your password?](#)

SIGN IN

Passwords resets are not breach disclosures!

Companies need to do a better job at letting their users control their own data. If there is a data breach, it is necessary for the companies to disclose this information so that users can adequately protect themselves.

Yet for the second time in a week, a company has decided that a password reset is their first step in disclosing a breach. First with StockX and now with CafePress.

Password reset notifications must be done at the same time as breach notifications.

Not before and not after.

Source: <https://www.bleepingcomputer.com/news/security/cafe-press-data-breach-exposes-personal-info-of-23-million-users/>

2. Leveraging AI to Win the Cybercrime Arms Race

Cybercriminals and cybersecurity professionals are caught in a perpetual game of one-upmanship when it comes to developing and deploying tools to either defend digital resources or exploit them. The latest entry in this ongoing cyber arms race is the use of automation, machine learning, and ultimately, Artificial Intelligence.

This isn't just science fiction. A recent report by Nokia, for example, showed that AI-powered botnets are being used to find specific vulnerabilities in Android devices and then exploit those vulnerabilities by loading data-stealing malware that is usually only detected after the damage has been done.

The Digital Transformation Challenge For Business

Digital transformation (DX) has managed to completely upend years of security strategy for cybersecurity professionals. However, due to the expansion of the cybersecurity skills gap, organizations simply cannot afford to scale their security infrastructure to address their growing attack surface.

Solving this challenge requires turning over lower order decisions and tedious processes to automated systems that require fewer eyes and hands. At the same time, traditionally isolated legacy security devices not only need to be exchanged for integrated systems that extend visibility and control across all network environments, but they need to include things like machine learning and AI to close gaps, correlate threat intelligence, and coordinate responses at digital speeds.

The Digital Transformation Opportunity For Cybercriminals

At the same time, DX has been one of the greatest boons to the cybercriminal community by multiplying the potential attack surface exponentially. AI and machine learning are just as helpful here as they are for enterprise networks.

As with their victims, maintaining ROI for a cybercriminal enterprise requires lowering overhead while increasing the efficiency and effectiveness of tools designed to penetrate defense systems.

For example, integrated malware that can run on a variety of devices and environments and deliver a variety of exploits and payloads is critical can be very effective. However, by leveraging automation and machine learning, that malware can autonomously determine which payloads will be most successful without exposing itself through constant communications back to its C2 server. The result is more effective data attempts without increasing overhead.

AI Takes Everything To The Next Level

Attacks that leverage self-learning technologies can quickly assess vulnerabilities, select or adapt malware, and actively counter security efforts to stop them. Combining AI with emerging threats like swarmbots will enable an attack to be broken down into its functional elements, assign them to different members of a swarm, and use interactive communications across the swarm to accelerate the rate at which an attack can occur.

The only effective defense against such AI-enhanced attacks strategies are solutions that use those same strategies.

“AI will allow businesses to deploy a self-defending security solution that can detect threats, close gaps, reconfigure devices and respond to threats without human intervention.”

– Derek Manky, SC Magazine, May 30, 2019

Because so many vendors see all the potential revenue associated with AI, many have been willing to claim AI functionality where it doesn't actually exist, which can leave those enterprises looking to “fight fire with fire” in a quandary as to which solutions they should select.

To cut through the confusion, IT teams need to ask security vendors a handful of questions to determine whether their AI solution is even worth considering:

How many years have you spent developing this AI? AI requires years of careful training. Any vendor who has not used standards-based training over the course of years to train their AI system is offering a less than ideal solution.

How many nodes are used to process data and make decisions? Generally speaking, true AI requires millions of nodes combined with massive amounts of data feeds to generate accurate defense solutions.

How good is the data you are feeding your AI? Feeding an AI with good data is harder than it sounds. Massive data sets of reliable and constantly available data is absolutely necessary for effective AI.

Fighting Fire With Fire

Not all AI is the same. Solutions that claim to provide AI but that don't meet the requirements listed above are likely to introduce more challenges into your network.

“Risk-based decision-making engines that are intelligent enough to take humans out of the loop not only need to be able to execute the “OODA loop” (Observe, Orient, Decide and Act) for the vast majority of situations it encounters, but also actually suggest courses of action when a problem is discovered rather than merely relying on pre-defined ones.”

– Derek Manky, SC Magazine, May 30, 2019

Locating tools that can meet that standard requires time and careful analysis. Only then can you confidently turn over critical security processes so your valuable cybersecurity experts can concentrate on those difficult decisions where human cognition and intervention are most required.

This is a summary of an article written for SC Magazine entitled, Winning the cybercrime arms race with AI, written by Fortinet’s Global Security Strategist, Derek Manky and published on Security Week on May 30, 2019.

Source: <http://feedproxy.google.com/~r/fortinet/blogs/~3/S2VHTC0wwHA/leverage-ai-to-win-cybercrime-arms-race.html>

3. 'Coordinated Ransomware Attack' in Texas Hits 23 Local Governments

Texas is currently fighting an unprecedented wave of ransomware attacks that has targeted local government entities in the state, with at least 23 impacted by the attacks.

Details are at a minimum at the moment as the Department of Information Resources (DIR) leads the response and investigation into the attacks. Texas released a brief notification advising affected local jurisdictions to call the state's Division of Emergency Management for assistance.

23 may not be the final count

The attacks started in the morning of August 16 and based on the collected evidence appear to have been conducted by a single threat actor.

The number of confirmed victims is 23 and the department believes that this is how many entities were "actually or potentially impacted;" all of them have been notified.

The origin of this attack is currently unknown, but is being investigated by local Texas authorities such as the DIR, Texas Division of Emergency Management, and Texas Military Department.

Also involved in the investigation are federal agencies such as the Department of Homeland Security, Federal Bureau of Investigation – Cyber, and Federal Emergency Management Agency (FEMA).

In its original statement released late Friday, DIR says that while investigations into the origins of the attack are ongoing, their main priority is to assist in the response and recovery of affected entities.

"Currently, DIR, the Texas Military Department, and the Texas A&M University System's Cyberresponse and Security Operations Center teams are deploying resources to the most critically impacted jurisdictions."

Additional resources will be provisioned if they are requested, DIR added, noting that the Texas Division of Emergency Management (TDEM) is assisting the effort by coordinating state agency support through state's operations center.

DIR is leading the response to what it calls a "coordinated ransomware attack" but does not disclose which organizations are impacted. This is because of security concerns.

Elliot Sprehe, press secretary for the department, told KUT, Austin's NPR Station that DIR was trying to confirm the total number of affected entities.

"It looks like we found out earlier today, but we're not currently releasing who's impacted due to security concerns," Sprehe told the public radio station.

In an updated statement on Saturday, DIR said that the systems and networks of the State of Texas have not been affected by this attack.

Until more details emerge, it remains unclear the strain of file-encrypting malware responsible for the attack and the perpetrator(s) ransom demand.

Hopefully, a proper backup system was implemented and current efforts to restore activity to normal relate only to recover the data from the safe copies.

Ransomware is big in U.S.

Ransomware incidents have increased lately in the U.S., and the government sector is a frequent target. And it makes sense when more and more administrative entities decide to pay the ransom, which may get as high as half a million dollars.

Telemetry data from security company Malwarebytes reveals the the U.S. has been at the receiving end of ransomware attacks more than any other country in the world, accounting for 53% of the global incidents.

In June, cybercriminals demanded and got paid in bitcoins worth a little over \$1 million at that time, from just two attacks in Florida.

Organizations in other states have also been hit by ransomware recently: the Town of Collierville in Tennessee, Onondaga County libraries in New York, Henry County in Georgia, school districts in Louisiana and Alabama.

The map below shows file-encrypting incidents impacting medical, educational and government organizations across the US:



What all these attacks should have in common is a backup restore procedure and not paying the cybercriminals.

Source: <https://www.bleepingcomputer.com/news/security/coordinated-ransomware-attack-in-texas-hits-23-local-governments/>

4. \$11M Email Scam at Caterpillar Sales Office Pinned to Nigerian Man

A Nigerian national that was on Forbes' list of the most promising entrepreneurs in Africa stands accused of business email compromise fraud that stole \$11 million from one victim alone.

Obinwanne Okeke is the founder of Invictus Group, involved in construction, agriculture, oil and gas, telecoms and real estate, according. In 2016, Forbes added him to its "Africa's 30 under 30" young business owners.

Fast forward three years later, the United States District Court for the Eastern District of Virginia issues an arrest warrant in Okeke's name for alleged conspiracies to commit computer and wire fraud.

Long time BEC scammer

According to the FBI affidavit in support of the criminal complaint and arrest warrant, Okeke had been running BEC scams since at least 2016, with some of his partners being involved in scams even before that.

With his co-conspirators, the fraudster worked on creating phishing pages for online services used by various businesses in the US.

In April 2018 Okeke and his associates sent a phishing email to the Chief Financial Officer (CFO) of Unatrac Holding Limited, which is the export sales office for Caterpillar industrial and farming equipment.

The CFO fell for the phishing and sent the login credentials to the fraudsters when they tried to access the email account in Microsoft Office 365.

"Logs indicate that between April 6 and April 20, 2018, the intruder accessed the CFO's account at least 464 times, mostly from Internet Protocol (IP) addresses in Nigeria" reads the affidavit from an FBI agent.

Tricks of the trade

With this level of access, it is stated that Okeke used the CFO's account to send fraudulent wire transfer requests to members of the company's internal financial team.

Some emails had fake invoices with Unatrac logos, while others had been sent to the CFO's account from an external email (pakfei.trade@gmail.com) and then forwarded to employees in charge of making payments, to create the appearance of a legitimate trail.

The affidavit states that the intruder created email filters that marked as read the legitimate emails from company employees and then moved them to a different folder. The purpose was to hide the replies from the receivers of fake invoices and fraudulent wire transfer requests.

In about a week between April 11 and April 19, 2018, Unatrac processed about 15 fraudulent payments. One recipient, Pak Fei Trade Limited, got three payments this way: for \$278,270, for \$898,461, and one for \$1,957,100.

In total, Unatrac sent nearly \$11 million to overseas accounts, and most of it could not be recovered.

Wrapping things up

The FBI allegedly linked Okeke to this fraudulent activity starting from the email address 'iconoclastlast1960@gmail.com,' which received files from Unatrac's CFO OneDrive storage account.

Following its trail on the internet, the FBI was able to uncover conversations with other fraudsters where they planned how to create new phishing pages. The email address also led to domain names that impersonated legitimate businesses and possibly used in other phishing campaigns.

Additional fraudulent domains were discovered, redacted in the affidavit. The breakthrough came from an FBI confidential source that linked 'iconoclastlast1960@gmail.com' malicious purposes.

Records from Google tied this address to other accounts that were accessed from the same machine, one of them being 'obinwannem@gmail.com,' linked to Okeke's '@invictusobi' Twitter profile. From there, it was a simple job tracking the real owner of the fraudulent account.

"The information Google provided lists a recovery email address of alibabaobi@gmail.com, and names several accounts linked to iconoclast1960@gmail.com by login session cookie, which indicates a likelihood that they are operated by the same person. One of these linked accounts is obinwannem@gmail.com"

Source: <https://www.bleepingcomputer.com/news/security/11m-email-scam-at-caterpillar-sales-office-pinned-to-nigerian-man/>

5. What Makes Local Government an Enticing Cyber Target?

Recent and well publicized cyber attacks are damaging, costly, and have the potential to deprive communities of essential services, but stopping them poses significant challenges.

Local government CISOs and IT departments face pressures from all sides: on the one hand, citizens are demanding digital services and frictionless online experiences, but on the other, government leaders want to reduce risk within the IT infrastructure, and face increasingly stringent data security compliance requirements. Moreover, limited budgets are always a reality.

Today's cybercriminals are savvy and well aware that local governments hold massive amounts of data. They're readily equipped to exploit that data's value, whether by selling it on the dark web, or through extortionary tactics like ransomware attacks.

Attractive Data

As local governments and municipalities are called upon to deliver services more efficiently, they're quickly expanding their technology infrastructures and the number of services they offer online. This means that their IT environments are growing rapidly and their complexity is skyrocketing. It also means that governments are collecting, storing, and transmitting ever-increasing amounts of sensitive data from their citizens.

Growing Cybersecurity Challenges

With these increasing services comes infrastructure sprawl and complexity. Many local governments now offer services via mobile or web applications, and a growing percentage of government organizations are turning to cloud-enabled storage or computing solutions. But, this IT modernization brings challenges: IT infrastructures are increasingly

distributed and heterogeneous, and attack surfaces correspondingly larger. At the same time, IT departments struggle to maintain visibility and control in these diverse environments.

In many ways, this creates the perfect storm for adversaries, and local governments' capacities for defense, response, and remediation are not always growing to keep pace with the size of the threat, due to some key challenges:

Breaking Down Silos

The agencies and departments comprising local governments often have highly-segregated organizational structures. This can make it difficult to develop centralized and consistent cybersecurity programs and standards, and implement them throughout the whole of the organization. Simply put, silos don't lend themselves to efficient collaboration. But stakeholders throughout all parts and segments of local government organizations must come together in support of a stronger cybersecurity posture—including greater awareness of the problem and better employee education—if there is to be real change.

Budget Constraints

Taxpayer-funded organizations like municipalities and local governments often have extremely limited resources. It's not uncommon for them to operate with legacy hardware or software, and a lack of technical security controls. In the current job market, cybersecurity talent is hard to come by, and salaries are high.

Ransomware is Top of Mind

The attacks on multiple cities, local governments, and education systems serve as a reminder that ransomware is not going away, but instead continues to pose a serious threat going forward. Ransomware attacks continue to move away from mass-volume, opportunistic attacks to more targeted attacks on organizations, which are perceived as having either the ability or the incentive to pay ransoms. In some instances, cybercriminals have conducted considerable reconnaissance before deploying their ransomware on carefully selected systems to maximize opportunity.

Regardless of the vector, as our latest Threat Landscape Report shows, ransomware continues to pose a serious threat for organizations going forward, serving as a reminder of the importance of prioritizing patching and infosecurity awareness education.

What's Needed: Simpler Security Solutions

In order for local governments and municipalities to continue their digital transformation initiatives without compromising on security, it's imperative that CISOs identify and deploy the security solutions that will enable them to make the best use of their limited resources. Not only must they compare the purchase and implementation costs of the technologies they're considering, but it's vital that they consider the management and administrative burden they would impose as well.

A consolidated, end-to-end solution offers significant advantages over an assortment of disparate point products. When local government IT departments adopt a fabric approach, it becomes easier to deploy and administer. If all components in the infrastructure can be managed through a central pane-of-glass interface, labor hours are much reduced, and costs will be a great deal lower.

In addition, integrated solutions are more effective, reducing overall risks. When devices are capable of sharing intelligence and taking automated action in response to threats, no component of the IT environment remains an island. Comprehensive solutions enable more seamless coverage, better visibility, and automated compliance reporting.

Source: <http://feedproxy.google.com/~r/fortinet/blogs/~3/En20Du1pGQs/state-local-government-cyber-target.html>

6. KuppingerCole Report on IT Landscape's Complexity

With every passing year, the landscape of data security becomes more crowded, more complex and, consequently, more challenging to manage.

According to an [Enterprise Strategy Group \(ESG\) survey](#) that polled IT decision-makers, 66 percent of respondents said IT is becoming more difficult than it was two years ago. The added challenge is attributable to the explosion of new types and sources of data that have emerged over the last few years. Similarly, when Forrester conducted its "[Global Business Technographics Security Survey](#)" last year, it found that, in addition to the ever-shifting nature of threats, 31 percent of business and IT decision-makers cited the complexity of the IT landscape as one of their biggest security challenges.

Defining Data Protection in an Age of IT Complexity

The traditional response to coping with this complexity has been for chief information security officers (CISOs) to purchase and deploy an ever-expanding arsenal of security software and hire more staff to implement those solutions. Enterprises employ as many as 80 distinct security products to meet their security needs, according to an estimate by IBM. However, this plan is not scalable in the long run. Even organizations that consider [data security](#) as mission-critical to their core business — financial services, healthcare companies and government agencies, to name a few — will ultimately face budgetary constraints when it comes to data security.

KuppingerCole, in its first Leadership Compass report published in two years on database and big data security, reflects this new reality. In the introduction, KuppingerCole recognizes the shift that has occurred in the market over the last two years: "A notable change in the direction the market is evolving has become apparent: as the amount and

variety of digital information an organization is managing grows, the complexity of the IT infrastructure needed to support this digital transformation grows as well.”

[Download the KuppingerCole Leadership Compass on Database and Big Data Security](#)

In its previous report, published in March 2017, KuppingerCole identified each of the key functional areas of data and database security solutions available when determining their ratings, breaking the market into eight distinct categories. This year, the report’s authors decided to forego a specific breakdown in favor of a more holistic view of the category, writing that “because of the broad range of technologies involved in ensuring comprehensive data protection, the scope of this market segment isn’t easy to define unambiguously.”

A Leader in Database and Big Data Security

So, how should business leaders and IT decision-makers meet the challenge posed by [mounting IT complexity](#)? Large-scale enterprise security companies offer integrated best-of-breed solutions across broad portfolios, providing solutions for myriad data protection pain points. Traditionally, these offerings focused on securing structured data, but the next frontier is securing unstructured data. Every hour, organizations produce a torrent of messages, documents, presentations and other unstructured data. In fact, the majority of data produced by organizations is unstructured, and much of it may contain business-sensitive information. Large enterprise security vendors have the breadth of portfolio, the cross-platform and integration capabilities, and, crucially, the development budget to conquer the mounting complexity.

With that in mind, it comes as no surprise that KuppingerCole listed [IBM Security Guardium](#) as a leader in the Database and Big Data Security category. In rating IBM as a “strong positive” in all five of its categories (Security, Functionality, Integration, Interoperability and Usability), KuppingerCole cited the breadth of Guardium’s portfolio, its support for hybrid multicloud environments and its nearly unlimited scalability as some of its greatest strengths.

All signs indicate that, with its broad and sophisticated portfolio, superior data discovery and classification system, and automated data compliance and audit capabilities, IBM Security Guardium is well-positioned to meet the critical challenges of the ever-changing, ever-expanding IT landscape.

Source: <http://feedproxy.google.com/~r/SecurityIntelligence/~3/z7eRZcKW2zE/>

7. How to Prepare for Misconfigurations Clouding the Corporate Skies

With cloud misconfigurations rampant in cloud storage and IaaS environments, adding security layers to identify them is crucial for securing sensitive data.

Cloud-based storage and infrastructure provides myriad benefits for any organization, like letting them avoid the costs of expensive hardware and granting them quick access to infrastructure as needed. Companies can use cloud services for minutes or years, depending on their needs. However, there is a darker side to this picture, in which cybercriminals can take advantage of the cloud if the infrastructure is not set up correctly and secured.

According to the Cloud Adoption & Risk Report released by McAfee earlier this year, there has been a 27.7 percent increase in cloud-related security incidents from the last year. With 65 percent of organizations using some form of an infrastructure-as-a-service (IaaS) model, organizations need to be aware of the risks that cloud-based options bring, and ensure that security is a top priority when deploying them.

Many people believe data security is the purview of cloud provider platforms like Amazon Web Services (AWS) and Microsoft's Azure. But AWS and others use a shared-responsibility model: Amazon takes the responsibility of securing its infrastructure, but the customer is responsible for configuring their environment securely. This includes ensuring that data is not shared inappropriately, identifying when a system is misused and enforcing compliance and/or governance policies (e.g., GDPR, PCI DSS, etc.).

As the McAfee report shows, the shared responsibility model for IaaS requires organizations to secure user access, data, applications, operating systems and network traffic. This leaves just the hypervisor, infrastructure, and physical systems up to the provider to secure.

This situation has led to a number of exposures and breaches of sensitive data because of an oversight on the part of cloud customers. For instance, in the Capital One data breach in July 2019, the financial giant used secure AWS as a platform, but a misconfiguration coupled with an ill-intending former employee of Amazon resulted in a massive data breach. About 140,000 Social Security numbers, 80,000 bank account numbers and details from more than 100 million consumer-credit applications were compromised.

Capital One's cloud-related breach isn't uncommon. In 2010, Microsoft had a breach in its Business Productivity Online Suite (BPOS). Like the Capital One breach, Microsoft's was also the result of a configuration issue in Microsoft's data centers. And since this incident, the misconfiguration problem has snowballed, with multiple data exposures every month being reported from companies of all stripes.

The stakes are high: One misconfigured server is all it takes, and the door is wide open for cybercriminals to steal all kinds of data. There are other dangers too: Cybercriminals that utilize Magecart malware have been automatically compromising domains and websites with credit-card skimmers by actively scanning for misconfigured Amazon S3 buckets.

Setting Up the Cloud

The biggest problem is that when deploying cloud environments, many pieces need to be configured, including the routing and firewall rules that grant access to the servers being deployed, the servers themselves, and the application-level firewalls and access rules within those servers. With so many components, and with effectively non-existent security in most default configurations, it is easy to see why one or more components may be deployed in an insecure state.

Even when users go through these configurations, some settings (like access control lists or ACLs) can be extremely long and complex to manage. This means that extensive testing is required to validate each rule. When time is insufficient, insecure settings may persist. According to the Cloud Security Alliance's report *Top Threats to Cloud Computing: Egregious Eleven*, "[a]n absence of effective change control is a common cause of misconfiguration in a cloud environment. Cloud environments and cloud computing methodologies differ from traditional information technology (IT) in ways that make changes more difficult to control."

This is because unlike in on-premise deployments, "infrastructure elements that were static in the corporate data center are now abstracted to software in the cloud."

Securing the Cloud from Stormy Weather

Misconfigurations may be common, but now that 21 percent of files in the cloud contain sensitive information, businesses must improve their data-security game with a multi-point security approach.

Generally speaking, network traffic analytics and user behavioral analysis can be used to spot anomalies that can alert IT to misconfigurations – as well as exposures that occur due to misconfigurations.

Since cloud platforms are inherently network-connected deployments, network traffic is a major way to understand how data is moving across these systems. In the case of AWS, Virtual Private Cloud (VPC) log information provides a clear picture of how data traverses Amazon's network to individual systems within AWS.

But VPC logs don't provide a complete picture if the system can be accessed outside the corporate network. Organizations must also ensure that access to cloud systems is restricted to individuals that authorized to tap into specific data on the corporate network. By requiring individuals to be physically present and authenticated on the network, organizations can track user behavior from everyone on the network.

When physical presence isn't possible, such as with remote employees, organizations should require employees to log on through the corporate VPN or other service that requires proper authentication (single sign-on, token validations, valid user credentials for corporate access, etc.), before connecting to corporate resources.

Meanwhile, network analysis alerts organizations when employees communicate with cloud systems they don't regularly connect to, and it allows security teams to spot potentially unauthorized access when a new connection takes place.

For example, it would be strange to have members of human resources or marketing connecting to a cloud system that maintains research and development resources, especially if the individual has never connected to the system before. In such instances, security teams can identify misconfigurations — and also any additional problems like stolen employee credentials, rogue employees and malware, based on the network traffic patterns.

Finding the Data Leak in the Cloud

As mentioned, network traffic can be a foundational resource for finding misconfigurations. While ACLs are crucial to stopping unauthorized connections, network traffic should also be used to verify that the rules are working as intended.

By seeing how resources communicate with one another, network and security teams can see when rogue agents are connecting to privileged resources or violating firewall rules. When security protocols are in place, and network traffic can verify that no unauthorized connections are taking place, businesses can verify that their cloud deployments are functioning as intended.

As the number of connections and the threat landscape grow, businesses must ensure their cloud buckets are properly configured, and that users are not abusing systems or being granted unauthorized access. Adding a few extra layers of security can go a long way in that effort.

Source: <https://threatpost.com/how-to-prepare-for-misconfigurations-that-cloud-the-corporate-skies/147538/>

8. Visa Adds New Threat Detection to Prevent Payment Fraud

Visa announced the addition of new fraud threat detection and blocking tech designed to boost transaction security and, implicitly, the integrity of its payments ecosystem.

The company's new payment fraud prevention security capabilities make it possible for financial institutions and merchant clients using its global electronic payments network.

All the security capabilities announced today are immediately available to all Visa clients, with no sign-up requirements or any additional costs.

"Cybercriminals attempt to bypass traditional defenses by stealing credentials, harvesting data, obtaining privileged access, and attacking trusted third-party supply chains," said RL Prasad, Visa Payment System Risk SVP.

New fraud detection capabilities

The new payment fraud detection tech Visa just added to its payments network is designed to protect its core components, namely the people, the data, and the infrastructure, to maintain the trust present at the center of all payment transactions.

Visa Vital Signs is the first of the four security additions and it is designed to constantly monitor all transactions throughout the network, automatically notifying "financial institutions of potential fraudulent activity at ATMs and merchants that may indicate an ATM cashout attack."

This new feature makes it possible for Visa to work in cooperation with its clients to quickly stop any malicious activity to minimize potential financial damages impacting partner financial institutions.

Visa Account Attack Intelligence uses deep learning to analyze the huge number of processed card-not-present transactions on Visa's database, to detect attackers' attempts to guess clients' account numbers, expiration dates, and security codes via automated testing.

The machine learning tech included with this new security feature "detects sophisticated enumeration patterns, eliminates false positives, and alerts affected financial institutions and merchants before fraudulent transactions begin."

Visa Payment Threats Lab allows the company to quickly set up a testing environment designed to examine any "client's processing, business logic and configuration settings" to pinpoint any flaws that could lead to new attack vectors.

For instance, "[Visa] verify if a financial institution is effectively validating cryptograms—dynamically generated codes unique to each transaction—for EMV chip transactions."

Last but not least, Visa eCommerce Threat Disruption (eTD) is a new and proprietary software which scans the front-end of eCommerce websites in real-time to trace payment card data skimmer malware, with the online stores of all merchants which accept Visa cards being automatically included.

This enables the company to actively reduce the amount of time its eCommerce clients and their customers are exposed to payment data skimmers, as well as drastically decrease the number of transactions which would be otherwise compromised by malicious campaigns using card skimmer scripts.

All these newly added security capabilities to Visa' payments network are designed to complement the real-time Visa Threat Intelligence (VTI) platform designed to protect clients from cyberattacks targeting payment data.

"Visa's new payment security capabilities combine payment and cyber intelligence, insights and learnings from breach investigations, and law enforcement engagement to help financial institutions and merchants solve the most critical security challenges," added Prasad.

Source: <https://www.bleepingcomputer.com/news/security/visa-adds-new-threat-detection-to-prevent-payment-fraud/>

9. PokerTracker.com Hacked to Inject Payment Card Stealing Script

A curious case of web-based card skimming activity revealed that the Poker Tracker website had been compromised and loaded JavaScript that stole payment information from customers.

Online poker enthusiasts use the Poker Tracker software suite to improve their winning chances by making decisions based on statistics compiled from the opponents' gameplay.

Magecart loading in poker app

A report on August 8 indicated that Malwarebytes anti-malware blocked Poker Tracker from connecting to a domain known to host credit card skimmers - scripts that copy payment card details on checkout pages and delivers them to the attacker.

Security researchers decided to investigate and after installing and running the software they noticed the same behavior: a connection to `ajaxclick[.]com` and retrieval of a malicious JavaScript file.

One early theory was that the application had been compromised. This would have been an unusual development for web skimmers since their presence has been observed only on websites.

However, a closer look at the software showed that it can load and display web pages from the PokerTracker subdomain 'pt4.pokertracker.com.'

Both sources had been hacked and injected with the malicious code causing the software to load it at every launch. Any payment made through the application or its website would copy the attacker with the payment details.

Outdated CMS

The compromise was possible because PokerTracker.com was running Drupal 6.3.x, an outdated version that has security vulnerabilities. The latest release for the platform is 8.6.17, available since June 17.

Jérôme Segura says that seeing this type of scripts targeting Drupal was surprising since the focus is typically on e-commerce platforms, Magento in particular.

After decoding the script (click.js), the data exfiltration process became clear. The data is verified before being serialized and encrypted with an easy to crack password: 'love1234.' The final stage is sending the data to the attacker's site.

The researcher notes that the skimmer was customized for this particular target, with variable names matching the input fields on the website, and the data segment in the code had PokerTracker.com hardcoded in.

Looking at the attacker's server, Segura found multiple skimmers all of them customized for each victim.

The owners of PokerTracker have been contacted and they acted promptly to fix the problem.

Malwarebytes was told that the site has improved the Content Security Policy (CSP), a web security standard that allows controlling the resources loaded for specific web pages.

Source: <https://www.bleepingcomputer.com/news/security/pokertrackercom-hacked-to-inject-payment-card-stealing-script/>

10. Agent 1433: remote attack on Microsoft SQL Server



All over the world companies large and small use Microsoft SQL Server for database management. Highly popular yet insufficiently protected, this DBMS is a target of choice

for hacking. One of the most common attack on Microsoft SQL Server — the remote attack based on malicious jobs — has been around for a long time, but it is still used to get access to workstations through less-than-strong administrator password.

Attempted attacks geography from January through July 2019 ([download](#))

According to our statistics, the majority of such attacks fall on Vietnam (>16%), Russia (~12%), India (~7%), China (~6%), Turkey and Brazil (5% each).

Attack description

Microsoft SQL Server attacks are normally massive in nature and have no particular target: the attackers scan sub-networks in search of a server with a weak password. The attack begins with a remote check of whether the system has MS SQL Server installed; next the intruders proceed to brute-force the account password to access the system. In addition to password brute-forcing, they may also resort to authorization via a user account token, authorized on a previously infected machine.

```
sub_401D56(&v6, "DRIVER={SQL Server};SERVER=");
v11 = 0;
sub_41DF18(v4 + 26);
sub_41DF18(",1433;Trusted_Connection=Yes;DATABASE=master");
LOBYTE(v11) = 1;
(*(void (__thiscall **)(_DWORD *, char *))(*v4[42] + 20))(v4[42], &v6);
sub_401D56(&v9, "SSPI");
LOBYTE(v11) = 2;
sub_401D56(&v8, "IntegratedSecurity");
```

SQL Server authorization

As soon as penetration is accomplished, the attackers [modify server configuration](#) in order to access the command line. That done, they can covertly make the malware secure in the target system using jobs they had created for the SQL Server.

Examples of jobs

Job is a sequence of commands executed by SQL Server agent. It may comprise a broad range of actions, including launching SQL transactions, command line applications, Microsoft ActiveX scripts, Integration Services packages, Analysis Services commands and queries, as well as PowerShell scripts.

A job consists of steps, the code featured in each one being executed at certain intervals, allowing intruders to deliver malicious files to the target computer again and again, should they be deleted.

Below are a few examples of malicious queries:

- Installing a malware download job using the standard ftp.exe utility:

- PDM:Trojan.Win32.GenAutorunSqlAgentJobRun.*
- PDM:Trojan.Win32.Generic
- PDM:Exploit.Win32.Generic

MD5

- 6754FA8C783A947414CE6591D6FA8540
- 91A12A4CF437589BA70B1687F5ACAD19
- 98DFA71C361283C4A1509C42F212FB0D
- A3F0B689C7CCFDFAEADD7CBBF1CD92B6
- E2A34F1D48CE4BE330F194E8AEFE9A55

Source: <https://securelist.com/malicious-tasks-in-ms-sql-server/92167/>

11. Asruex Backdoor Variant Infects Word and PDFs Through Old Vulnerabilities

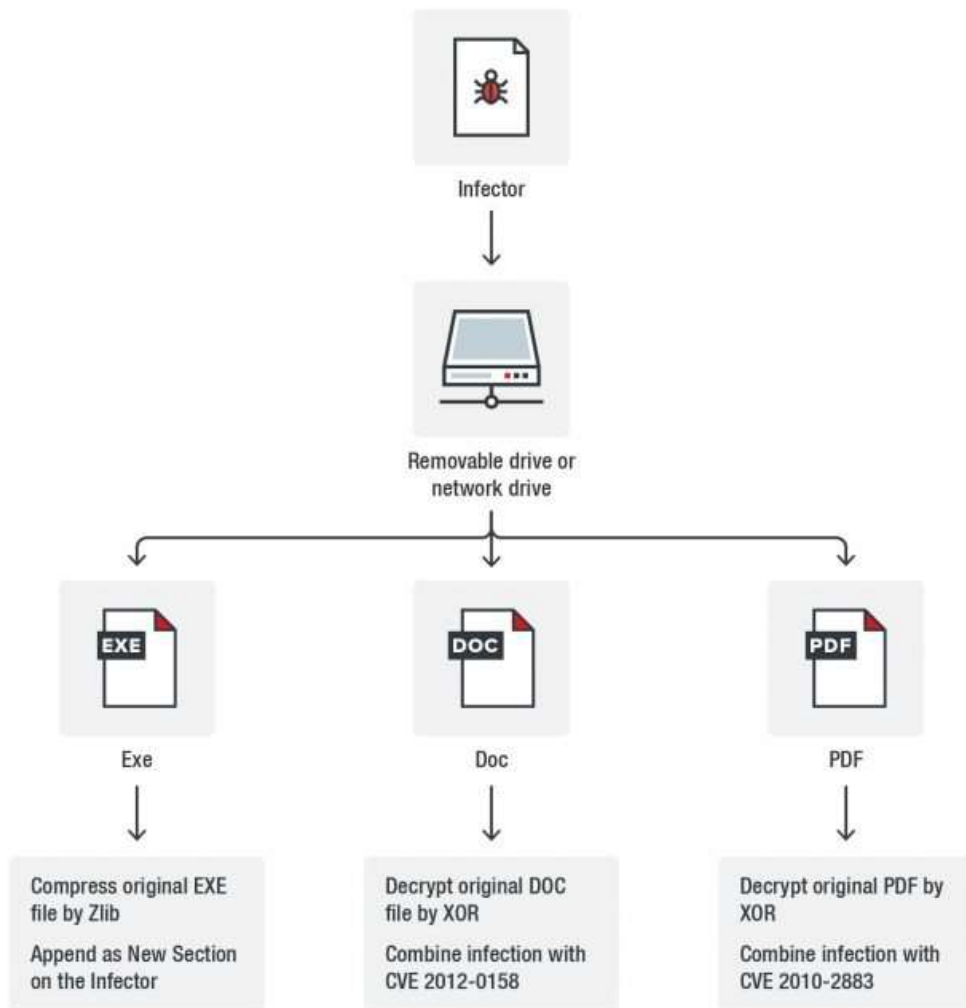
Since it first emerged in 2015, Asruex has been known for its [backdoor capabilities](#) and connection to the spyware DarkHotel. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities [CVE-2012-0158](#) and [CVE-2010-2883](#), which inject code in Word and PDF files respectively.

The use of old, patched vulnerabilities could hint that the variant was devised knowing that it can affect targets who have been using older versions of Adobe Reader (versions 9.x up to before 9.4) and Acrobat (versions 8.x up to before 8.2.5) on Windows and Mac OS X.

Because of this unique infection capability, security researchers might not consider checking files for an Asruex infection and continue to watch out for its backdoor abilities exclusively. Awareness of this new infection method could help users defend against the malware variant.

Technical details

Asruex infects a system through a shortcut file that has a PowerShell download script, and spreads through removable drives and network drives. The diagram below illustrates the malware's infection chain.



©2019 TRENDS MICRO

Infection chain of Asruex

Infected PDF files

We first encountered this variant as a PDF file. Further investigation revealed that the PDF file itself was not a malicious file created by the actors behind this variant. It was simply a file infected by the Asruex variant.

Infected PDF files would drop and execute the infector in the background if executed using older versions of Adobe Reader and Adobe Acrobat. As it does so it still displays or opens the content of the original PDF host file. This tricks the user into believing that the PDF had acted normally.

This behavior is due to a specially crafted template that takes advantage of the CVE -2010-2883 vulnerability while appending the host file. The vulnerability is found in the `strcat` function of Adobe's `CoolType.dll`, which is a typography engine. Since this function does not check the length of the font to be registered, it can cause a stack buffer overflow to

execute its shellcode. Finally, it decrypts the original PDF host file using XOR. This process is seen in the images below.

```

0803BD25 8D45 00 LEA EAX, DWORD PTR SS:[EBP] shellcode
0803BD28 50 PUSH EAX
0803BD29 C645 00 00 MOV BYTE PTR SS:[EBP], 0
0803BD2D E8 6C5B0100 CALL <JMP.&MSVCR80.strcat>

```

Vulnerability being exploited by the variant

```

01E1016C 304C0B FF XOR BYTE PTR DS:[EBX+ECX-1], CL
01E10170 ^ E2 FA LOOPD SHORT 01E1016C

```

```

00 00 00 00 00 00 00 00 25 50 44 46 2D 31 2E 34 .....%PDF-1.4
0A 25 E2 E3 CF D3 0A 34 20 30 20 6F 62 6A 0A 3C .%ääIö.4 0 obj.<
3C 2F 54 79 70 65 2F 58 4F 62 6A 65 63 74 0A 2F </Type/Xobject./
53 75 62 74 79 70 65 2F 49 6D 61 67 65 0A 2F 57 subtype/Image./w
69 64 74 68 20 33 35 30 38 0A 2F 48 65 69 67 68 idth 3508./Heigh
74 20 34 39 36 31 0A 2F 42 69 74 73 50 65 72 43 t 4961./BitsPerC
6F 6D 70 6F 6E 65 6E 74 20 38 0A 2F 43 6F 6C 6F omponent 8./Colo
72 53 70 61 63 65 2F 44 65 76 69 63 65 52 47 42 rSpace/DeviceRGB
0A 2F 46 69 6C 74 65 72 20 2F 44 43 54 44 65 63 ./Filter /DCTDec
6F 64 65 0A 2F 4C 65 6E 67 74 68 20 37 37 35 38 ode./Length 7758
30 30 0A 3E 3E 0A 73 74 72 65 61 6D 0A FF D8 FF 00.>>.stream.yöÿ
E0 00 10 4A 46 49 46 00 01 01 01 01 2C 01 2C 00 à.+JFIF.

```

Decrypting the original PDF host file

It will then drop and execute the embedded executable detected as Virus.Win32.ASRUEX.A.orig, as seen in figure 4.

```

01E101E8 CALL to winExec from 01E101E5
0C0C0B50 CmdLine = "cmd.exe /c ""C:\Users\win7x32\AppData\Local\Temp\ARB77E8.JPEG"
00000000 ShowState = SW_HIDE

```

The embedded executable dropped by the malware

This executable is responsible for several anti-debugging and anti-emulation functions. It detects if avast! Sandbox\WINDOWS\system32\kernel32.dll exists on any root, as an anti-debugging measure. It then checks the following information (listed below), to determine if it is running in a sandbox environment:

- Computer names and user names
- Exported functions by loaded modules
- File names
- Running processes
- Module version of running process
- Certain strings in disk names

The executable file also injects the DLL c982d2ab066c80f314af80dd5ba37ff9dd99288f (detected as Virus.Win32.ASRUEX.A.orig) into a legitimate Windows process memory. This

DLL is responsible for the malware’s infection and backdoor capabilities. It infects files with file sizes between 42,224 bytes and 20,971,520 bytes, possibly as a parameter to narrow down host files into which their malware code could fit.



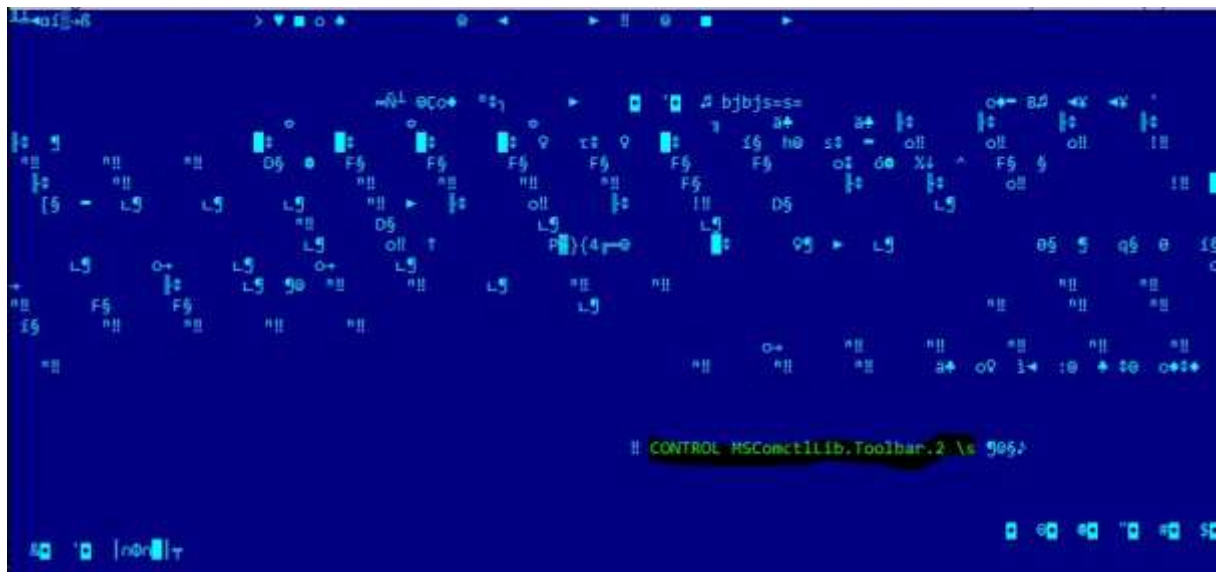
Screenshot showing the added process



Template that the infector uses to infect PDF samples; the filename of the executable is highlighted

Infected Word documents

As mentioned earlier, it uses a specially crafted template to exploit the CVE-2012-0158 vulnerability to infect Word documents. The template is highlighted in figure 7.



Template used to infect Word documents

The CVE-2012-0158 vulnerability allows possible attackers to execute an arbitrary code remotely through a Word document or web site. Similar to infected PDFs, it will drop and execute the infector in the background upon execution of the infected Word document file. At the same time, it will display the original DOC host file, letting users believe that the opened document is normal.

The infected file would use XOR to decrypt the original DOC host file, as seen in figure 8. The file would open like normal, with the only difference found in the filename used by the infector. It drops and executes itself as rundll32.exe (figure 9).

```
00121DBA 304C0B FF XOR BYTE PTR DS:[EBX+ECX-1],CL
00121DBE E2 FA LOOPD SHORT 00121DBA
```

Figure 8. Use of an XOR to decrypt the original DOC host file

```
00121548 00121EE6 CALL to WinExec from 00121EE3
0012154C 00121575 CmdLine = "C:\DOCUME~1\WINXP~1.KAR\LOCALS~1\Temp\rundll32.exe"
00121550 00000000 ShowState = SW_HIDE
00121554 2F646F63
```

Figure 9. Use of a different file name to drop and execute the infector

Infected executables

Aside from the Word documents and PDF files, the malware also infects executable files. This Asruex variant compresses and encrypts the original executable file or host file and appends it as its .EBSS section. This allows the malware to drop the infector, while also executing the host file like normal. For infected executable files, the filename used by the infector when dropped is randomly assigned, as illustrated in figure 11.

Conclusion and security recommendations

As mentioned earlier, past reports have tagged Asruex for its [backdoor capabilities](#). The discovery of this particular infection capability can help create adequate defenses against the malware variant.

This case is notable for its use of vulnerabilities that have been discovered (and patched) over five years ago, when we've been seeing this malware variant in the wild for only a year. This hints that the cybercriminals behind it had devised the variant knowing that users have not yet patched or updated to newer versions of the Adobe Acrobat and Adobe Reader software.

Understandably, this could pose a challenge for organizations as updating widely-used software could result in downtime of critical servers, and it could be costly and time consuming. If patching and updating might not be a present option, organizations can consider security measures like [virtual patching](#) to help complement existing security measures and patch management processes.

In general, users can take the necessary measures to defend against similar threats by following security best practices. We list down some of the steps users can take to defend against Asruex and similar malware:

- Always scan removable drives before executing any file that may be stored in it.
- Avoid accessing suspicious or unknown URLs.
- Be cautious when opening or downloading email attachments, especially from unknown or unsolicited email.

Users and enterprises can also benefit from a solution that uses a multilayered approach against threats that are similar to Asruex. We recommend employing [endpoint application control](#) that reduces attack exposure by ensuring that only files, documents, and updates associated with whitelisted applications and sites can be installed, downloaded, and viewed. Endpoint solutions powered by [XGen™ security](#) such as [Trend Micro™ Security](#) and [Trend Micro Network Defense](#) can detect related malicious files and URLs and protect users' systems. [Trend Micro™ Smart Protection Suites](#) and [Trend Micro Worry-Free™ Business Security](#), which have [behavior monitoring capabilities](#), can additionally protect from these types of threats by detecting malicious files, as well as blocking all related malicious URLs.

Indicators of Compromise (IoCs)

SHA256

b261f49fb6574af0bef16765c3db2900a5d3ca24639e9717b
c21eb28e1e6be77

Detection Name

Virus.Win32.ASRUE
X.A.orig

The post [Asruex Backdoor Variant Infects Word Documents and PDFs Through Old MS Office and Adobe Vulnerabilities](#) appeared first on .

- ◆ [Email this](#)
- ◆ [Save to del.icio.us](#)
- ◆ [Share on Facebook](#)
- ◆ [Digg This!](#)
- ◆ [Discuss on Newsvine](#)
- ◆ [Add to Mixx!](#)

Source: <http://feeds.trendmicro.com/~r/Anti-MalwareBlog/~3/6obcYqeWkzM/>

12. Unpatched Squid Servers Exposed to DoS, Code Execution Attacks

Multiple versions of the Squid web proxy cache server built with Basic Authentication features are currently vulnerable to code execution and denial-of-service (DoS) attacks triggered by the exploitation of a heap buffer overflow security flaw.

The vulnerability present in Squid 4.0.23 through 4.7 is caused by incorrect buffer management which renders vulnerable installations to "a heap overflow and possible remote code execution attack when processing HTTP Authentication credentials."

"When checking Basic Authentication with `HTTPHeader::getAuth`, Squid uses a global buffer to store the decoded data," says MITRE's description of the vulnerability. "Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data."

The flaw was patched by the web proxy's development team with the release of Squid 4.8 on July 9.

Some unpatched servers exposed to attacks

Remote unauthenticated attackers could exploit the flaw tracked as CVE-2019-12527 that comes with a high severity CVSS v3.0 base score of 8.8 by sending a specially crafted request to any targeted server to either execute arbitrary code or to cause Squid to crash, triggering a DoS state.

"A remote attacker can exploit this vulnerability by sending a crafted HTTP request to the target server," details the Trend Micro Research Team in a write-up covering CVE-2019-12527.

"Successful exploitation will result in the attacker being able to execute arbitrary code with the privileges of the server process while an unsuccessful attack will cause the server process to abnormally terminate."

Luckily, according to the security advisory published by Squid's security team on July 12 after patching, "this issue is limited to traffic accessing the Squid Cache Manager reports or using the FTP protocol gateway."

Also, only unpatched "Squid-4.0.23 up to and including 4.7 built with Basic Authentication features are vulnerable" to attacks.



Top Countries	
1. United States	22,061
2. Honduras	7,352
3. Canada	2,137
4. Germany	257
5. Turkey	243
6. Brazil	122
7. Ireland	99
8. United Kingdom	94
9. Australia	70
10. Lithuania	58

Number of unpatched Squid 4.7 servers by country

The Squid security advisory recommends the following workarounds for servers that can't be patched:

Deny ftp:// protocol URLs being proxied and Cache Manager report access to all clients:

```
acl FTP proto FTP
http_access deny FTP
http_access deny manager
```

Or,

Build Squid with *--disable-auth-basic*

Servers still vulnerable, two more flaws patched

Even though the vulnerability was patched back in early July, out of a total 2,776,255 of exposed Squid servers found using the Shodan search engine, 31,576 are still running 4.7 (the last vulnerable version), with only 1,956 having been upgraded to the 4.8 patched release.

To have an idea of the number of servers potentially exposed to attacks, we have compiled a list of all vulnerable Squid versions and the current number of servers found with Shodan in the table available below.

Vulnerable version	Number of exposed servers
4.7	31576
4.6	1314
4.5	108
4.4	7439
4.3	35
4.2	885
4.1	2244
4.0.25	4
4.0.24	78
4.0.23	294

Total number of unpatched servers **43977**

While not all of the over 43,000 servers found to be unpatched are vulnerable, the number can easily reach thousands depending on how many of them run installations that have been built with Basic Authentication features.

The Squid 4.8 release also patched a critical flaw tracked as CVE-2019-12525 found in Squid 3.3.9 through 3.5.28 and 4.x through 4.7, and the medium severity CVE-2019-12529 present in Squid 2.x through 2.7. STABLE9, 3.x through 3.5.28, and 4.x through 4.7.

Remote attackers who would exploit one these two Squid security flaws can cause the target Squid servers to crash, triggering a DoS state for all clients using the proxy.

"Squid is a high-performance proxy caching server for web clients, supporting FTP, gopher, and HTTP data objects," says its wiki, "Squid handles all requests in a single, non-blocking, I/O-driven process over IPv4 or IPv6."

"Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests."

Source: <https://www.bleepingcomputer.com/news/security/unpatched-squid-servers-exposed-to-dos-code-execution-attacks/>

13. ThreatList: Half of All Social Media Logins Are Fraud

Fraudsters are using social media to spam, steal information, spread propaganda and execute social-engineering campaigns.

More than half of logins (53 percent) on social-media sites are fraudulent; and 25 percent of all new account applications on social media are fake, according to a recent analysis. Those numbers far outstrip the overall rate of 10 percent of interactions being fraudulent.

The Arkose Labs Q3 Fraud and Abuse Report found that social-media platforms see a variety of attacks from bots as well as malicious humans, including account takeovers, fraudulent account creation, spam and other abuse. More than three-quarters (75 percent) of attacks on social media are automated bot attacks, according to the analysis.

Unlike other industries, account-takeover attacks are more common for social media, with logins twice as likely to be attacked than account registrations. This is driven by the fraudsters looking to harvest rich personal data from the accounts of legitimate users, according to Arkose.

"The extremely high attack rate on social-media logins is indicative of the value placed on the data fraudsters extract from compromised social accounts," said Kevin Gosschalk, CEO of Arkose, in a media statement. "Because more than 50 percent of social media logins

are fraud, we know that fraudsters are using large-scale bots to launch attacks on social-media platforms with the goal of disseminating spam, stealing information, spreading social propaganda and executing social-engineering campaigns targeting trusting consumers.”

From an overall digital fraud perspective, Arkose examined more than 1.2 billion transactions spanning account registrations, logins and payments from financial services, e-commerce, travel, social media, gaming and entertainment industries, and found that one in 10 transactions overall are malicious, ranging from automated bots to humans carrying out scams.

Bots vs. Humans

Automated attacks represent the bulk of the traffic, according to the report, ranging from large-scale account validation attacks, to bots blocking seats on an airline to scripted attacks that scrape user data and inventory.

This varies by geography and industry though: Further analysis found that most attacks from China (59.3 percent) are human-driven, which is more than four times higher than the U.S., Russia, the Philippines, and Indonesia.

Unlike bot traffic, inauthentic human traffic is harder to detect as human behavior is unpredictable and highly nuanced.

“Sometimes fraudsters have to rely on humans to carry out attacks; these attacks cost more, but the value they can extract from the attack makes the investment worthwhile,” said Vanita Pandey, vice president of strategy at Arkose Labs, in a media statement. “Developing economies are quickly becoming fraud hubs because they have easy access to sophisticated tools, cheap manual labor and good economic incentives associated with online fraud.”

Attacks by Industry

The report pinpointed some interesting vertical trends: For one, payment transactions in the travel industry are 10 times more likely to be attacked; and, the retail industry experiences the highest volume of human driven attacks, with more than half of attacks being human-driven.

The travel industry attacks are mainly coming from automated bots looking to block inventory, leading to denial of inventory attacks or a significant increases in ticket prices. They’re also looking to steal hard-customer loyalty points, which can be liquidated into cash. Overall, Arkose Labs found that almost 10 percent of all login attempts on travel sites and 46 percent of all payment transactions for travel are fraud.

As for retail, the sector is on the cusp of the most-attacked time of the year.

“As we head into the holiday season, this is critical for the retail industry, which sees high volumes of seasonal and human driven fraud,” said Pandey. “Right now, fraudsters are

actively preparing to launch large-scale attacks on retail vendors during the holidays by validating and testing stolen gift cards and identities compromised in recent breaches. The long-term solution to this problem is not rooted in applying new defenses — because fraud will continue to evolve — but rather to break the economics of the attack and eliminate a fraudster’s financial incentive.”

Meanwhile, the technology segment is heavily targeted by human click-farms and sweatshops, which employ a large group of low-paid workers hired specifically to make fraudulent transactions or create fake accounts, the report found. In fact, 43 percent of all attacks on tech companies are human driven and account registrations for tech companies are four times more likely to be attacks than logins.

According to the report, the U.S., Russia, the Philippines, the UK and Indonesia have emerged as the top originators of attacks, with the Philippines as the single biggest attack originator for both automated and human-driven attacks. The U.S. is a distant second.

Source: <https://threatpost.com/half-social-media-logins-fraud/147688/>

14. Hostinger Data Breach: 14M Customer Passwords, Personal Data at Risk

Web hosting company Hostinger is warning that a breach of one of its servers potentially gave bad actors access to the hashed passwords and personal data of more than 14 million customers.

Hostinger, a popular web, cloud and virtual private server hosting provider and domain registrar with 29 million+ users, has notified customers that it has reset all passwords after the unauthorized third party gained access to an internal system API server. The server contained hashed passwords and other non-financial data about customers.

As of Sunday, the company said that it is working with internal and external forensic teams to analyze network and server logs: “We are continuing our internal review, implementing new security procedures and hardening server and network settings,” it said in a website notice.

Hostinger first became aware of the breach on Friday after receiving informational alerts that one of its servers had been accessed by an unauthorized third party.

“This server contained an authorization token, which was used to obtain further access and escalate privileges to our system RESTful API server,” said Hostinger. “This API server is used to query the details about our clients and their accounts.”

The API database included client usernames, emails, hashed passwords, first names and IP addresses. The table held the information about 14 million Hostinger users, researchers said. What isn’t impacted is financial data, Hostinger client website accounts and data stored on those accounts (websites, domains and hosted emails).

The company said it has identified the origin of unauthorized access and the vulnerable system has since been secured.

While the passwords were protected by the SHA-1 algorithm, that protection mechanism is not 100 percent effective and has been found vulnerable to collision attacks.

“Immediately following the security incident, all Hostinger user passwords have been reset using SHA-256 hashing algorithm,” a Hostinger spokesperson told Threatpost. “Prior to the security incident, SHA-1 hashing algorithm was used to hash user passwords.”

While Hostinger has reset impacted customer passwords, security experts are urging anyone impacted to ensure that their potentially compromised passwords aren’t being re-used elsewhere — an issue that still affects hundreds of thousands of internet users, a recent Google study found.

Tim Erlin, vice president of product management and strategy at Tripwire, told Threatpost that the incident points to how “password reuse is a real problem.”

“When password hashes are copied, the risk is that an attacker will be able to crack those passwords and then use the information to authenticate to the compromised service, or to other services where those passwords are used,” he said. “If you’ve used the same password in multiple places, you may never know when or how your password was compromised.”

Justin Fox, director of DevOps Engineering for NuData Security, added that enabling multi-factor authentication is a good way for service providers to mitigate the risk of a compromised password.

“Two-factor authentication can be combined with other security layers such as passive biometrics and behavioral analytics, so that if one layer fails, another layer of security takes over, protecting the customers’ accounts even if the credentials have been stolen,” he said in an email. “While two-factor authentication capabilities can help verify the user, behavioral analytics and passive biometrics allow you to learn and trust the user’s behavior both at login and across the session.”

Source: <https://threatpost.com/hostinger-data-breach-14m-passwords/147681/>

15. Malware Operation Making Millions Defeated by Design Flaw

The reign of Retadup botnet over more than 850,000 systems has reached an end as its command and control server (C2) was taken down by security researchers from antivirus maker Avast working with the French National Gendarmerie.

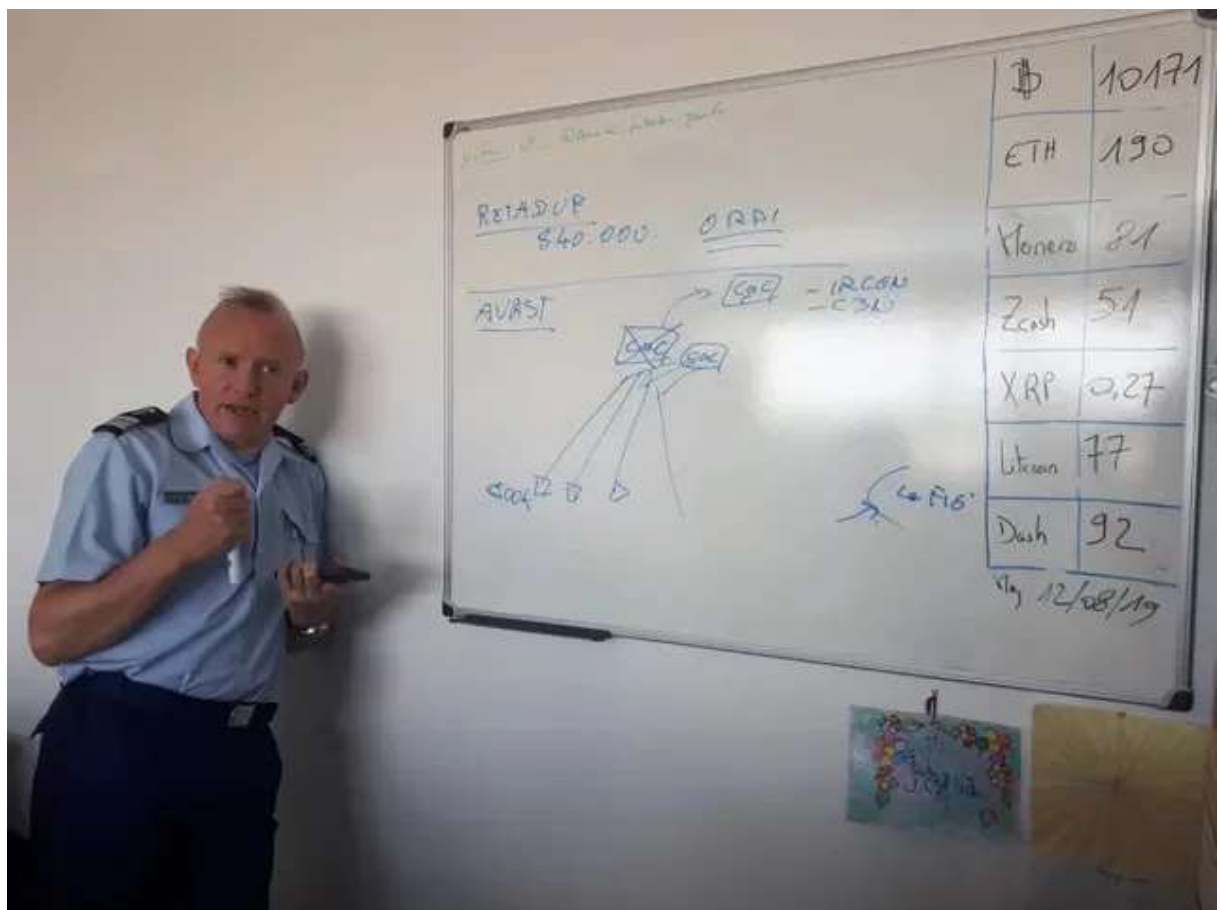
The botnet was mostly used for cryptojacking, the researchers say but it also spread the Stop ransomware and the Arkei info stealer.

Botnet handler(s) may have made millions

It is unclear how much money the operator(s) made, but one Monero address that Avast discovered on Retadup's C2 shows a month's profit above \$4,200 (XMR 53,72).

The figure is from just one mining pool, though, and configuration files show that the operator used others, too. Although the estimated monthly revenue is unclear, it is expected to be much more than this.

French public radio channel France Inter published an image of Jean-Dominique Nollet, head of the Cybercrime Fighting Center (C3N) of the French National Gendarmerie, discussing Retadup takedown that suggests huge profits for the botnet operators.



In an interview on the matter, Nollet said that the operators earned "several million euros" every year starting 2016.

Author leaves obvious traces

Details about the handlers of the botnet are not public at this time, but starting from a C2 domain published by Avast, one researcher was able to find information on the botnet's author upon investigating the report by avast

(https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/#cnc_domains ...) we started looking into the c&cs involved in the hack.

In a short amount of time, the researcher found a phone number, an email address, and a Facebook profile of someone claiming to be the developer of Retadup.

The individual appears to be a 26-year old who boasted their achievement through posts showing huge numbers of victims. A post from November 2016 brags about a victim count of 150,000.

On April 27, 2018, someone claiming authorship of the botnet published a snapshot from a controlling server showing close to 200,000 machines infected with Retadup.

Ironically, the image was in a reply to Trend Micro's first research on the malware. Researchers determined that the Twitter account belonged to the author and the information was genuine.

Most victims in Latin America

Public details on Retadup emerged in mid-2017 when it was found to distribute an information stealer to hospitals in Israel. It pretended to be an executable for updating Windows.

The main malware, however, was a backdoor with self-propagating capabilities. Its set of features included taking screenshots, installing a keylogger, starting/restarting/stopping processes, shutting down, restarting, or logging off the machine.

In a blog post today, Avast says that most Retadup victims were in Spanish-speaking countries, with Peru leading the pack with over 320,000 infections. In total, the malware compromised computers in 140 countries.

Design flaw brings botnet down

Bringing down the Redatup infrastructure was possible due to a design flaw that Avast found in the botnet's communication protocol. Once they took over the C2, the bug allowed the researchers to clean infected hosts without user intervention.

Although there were just a few hundred French victims, most of the botnet's infrastructure was located in France, so authorities in the country were contacted and presented the solution.

Once the prosecutor approved the plan, the Gendarmerie replaced the malicious C2 server with a version "that made connected instances of Retadup self-destruct."

"In the very first second of its activity, several thousand bots connected to it in order to fetch commands from the server." - Avast

In total, over 850,000 unique infections have been neutralized. Most of the machines were running Windows 7 and had two or four cores. Over 85% of the systems ran with the default antivirus solution.

Source: <https://www.bleepingcomputer.com/news/security/malware-operation-making-millions-defeated-by-design-flaw/>



If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.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 BUSINESS SERVICES 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 BUSINESS SERVICES'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 BUSINESS SERVICES 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.