E-BRIEF // JAN 31 2019

Intelligence vs Data

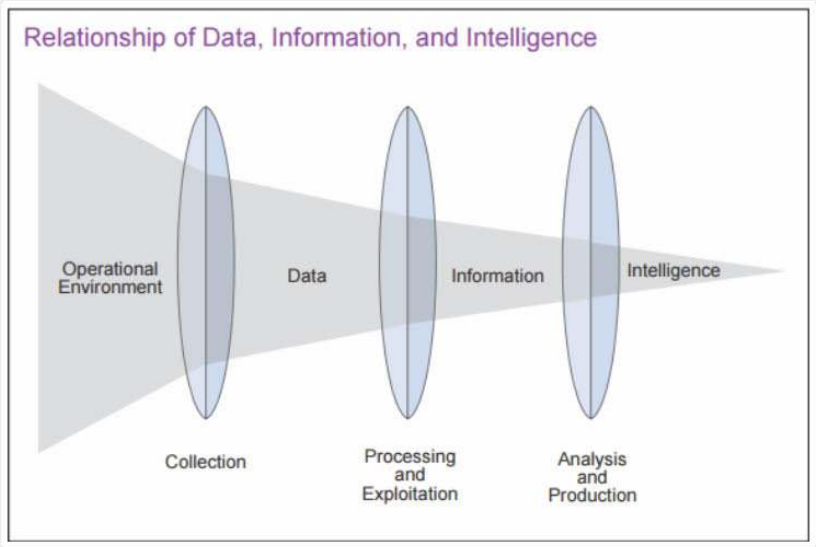
What is Intelligence?

Data is not information, information is not intelligence. While information consists of data points, its usefulness and applicability are limited unless it can be tied to a specific entity or event. Intelligence can be seen as information that has been correlated and aligned in relation to an entity or event that will affect or impact future actions or decision making.

Data, Information and Intelligence

A typical example provided by cyber security providers is an IP address, this is **data**. If that IP address is processed and has been shown to be associated with malicious activity that additional context is **information**. If analysis of that IP address shows traffic into or out of your organization then that information becomes **intelligence**.

The image below, taken from the Department of Defense Joint Publication 2.0 - Joint Intelligence, does a good job of showing the relationships of data, information and intelligence.



While the process identified above can result in intelligence and provide guidance or an actionable item there still may be too much collected and not everything needs to be addressed.

As part of the Intelligence Cycle, some direction and requirements will help to narrow down what needs to be addressed first or is more important to the organization. Is a competitor buying up real estate in a specific market more important than a malicious group targeting a specific industry?

By providing direction for intelligence requirements, the collection process and analysis will better align and support the organization's strategic objectives as well as providing actionable items that increase overall safety and security.

A majority of "intelligence feeds" , reports, and briefs (including this document) are not and should not be considered intelligence. While useful security events and information are provided, no analysis or correlation has been performed to a specific organization or individual that would result in being able to make a meaningful or beneficial decision or action.

Relevance through requirements and analysis leads to intelligent decisions.

China Hacked HPE, IBM And Then Attacked Clients

WASHINGTON/LONDON/SAN FRANCISCO (Reuters) - Hackers working on behalf of China's Ministry of State Security breached the networks of Hewlett Packard Enterprise Co and IBM, then used the access to hack into their clients' computers, according to five sources familiar with the attacks.

The attacks were part of a Chinese campaign known as Cloudhopper, which the United States and Britain on Thursday said infected technology service providers in order to steal secrets from their clients.

While cybersecurity firms and government agencies have issued multiple warnings about the Cloudhopper threat since 2017, they have not disclosed the identity of technology companies whose networks were compromised.

International Business Machines Corp said it had no evidence that sensitive corporate data had been compromised. Hewlett Packard Enterprise (HPE) said it could not comment on the Cloudhopper campaign.

Businesses and governments are increasingly looking to technology companies known as managed service providers (MSPs) to remotely manage their information technology operations, including servers, storage, networking and help-desk support.

Cloudhopper targeted MSPs to access client networks and steal corporate secrets from companies around the globe, according to a U.S. federal indictment of two Chinese nationals unsealed on Thursday. Prosecutors did not identify any of the MSPs that were breached.

Both IBM and HPE declined to comment on the specific claims made by the sources.

"IBM has been aware of the reported attacks and already has taken extensive counter-measures worldwide as part of our continuous efforts to protect the company and our clients against constantly evolving threats," the company said in a statement. "We take

responsible stewardship of client data very seriously, and have no evidence that sensitive IBM or client data has been compromised by this threat."

HPE said in a statement that it had spun out a large managed-services business in a 2017 merger with Computer Sciences Corp that formed a new company, DXC Technology.

"The security of HPE customer data is our top priority," HPE said. "We are unable to comment on the specific details described in the indictment, but HPE's managed services provider business moved to DXC Technology in connection with HPE's divestiture of its Enterprise Services business in 2017."

DXC Technology declined to comment, saying in a statement that it does not comment on reports about specific cyber events and hacking groups.

Reuters was unable to confirm the names of other breached technology firms or identify any affected clients.

The sources, who were not authorized to comment on confidential information gleaned from investigations into the hacks, said that HPE and IBM were not the only prominent technology companies whose networks had been compromised by Cloudhopper.

Cloudhopper, which has been targeting technology services providers for several years, infiltrated the networks of HPE and IBM multiple times in breaches that lasted for weeks and months, according to another of the sources with knowledge of the matter.

IBM investigated an attack as recently as this summer, and HPE conducted a large breach investigation in early 2017, the source said.

The attackers were persistent, making it difficult to ensure that networks were safe, said another source.

IBM has dealt with some infections by installing new hard drives and fresh operating systems on infected computers, said the person familiar with the effort.

Cloudhopper attacks date back to at least 2014, according the indictment.

The indictment cited one case in which Cloudhopper compromised data of an MSP in New York state and clients in 12 countries including Brazil, Germany, India, Japan, the United Arab Emirates, Britain and the United States. They were from industries including finance, electronics, medical equipment, biotechnology, automotive, mining, and oil and gas exploration.

One senior intelligence official, who declined to name any victims who were breached, said attacks on MSPs were a significant threat because they essentially turned technology companies into launchpads for hacks on clients.

“By gaining access to an MSP, you can in many cases gain access to any one of their customers,” said the official. “Call it the Walmart approach: If I needed to get 30 different items for my shopping list, I could go to 15 different stores or I could go to the one that has everything.”

Representatives with the FBI and Department of Homeland Security declined to comment. Officials with the U.S. Justice Department and the Chinese embassy in Washington could not be reached.

A British government spokeswoman declined to comment on the identities of companies affected by the Cloudhopper campaign or the impact of those breaches.

“A number of MSPs have been affected, and naming them would have potential commercial consequences for them, putting them at an unfair disadvantage to their competitors,” she said.

Source: Reuters

Pro-ISIS Media Organization Testing the “ZeroNet” Decentralized Peer-to-Peer Network

In a continued effort to maintain their online presence, pro-ISIS media organizations continue to test new Social Media Sites (SMS) and Mobile Messaging Applications (MMAs). Recent and historic incidents show that ISIS media accounts, both official and semi-official, are typically the first to test alternative platforms. Since 2017, Amaq Agency and Nashir News Agency (not to be confused with the official Arabic-language Nashir media) have consistently been the first to test new platforms.

On 14 January 2019, the pro-ISIS Al Battar Media Establishment posted an advertisement on their Telegram Channel for Amaq Agency’s ZeroNet Website. Two URLs were provided for Amaq Agency’s website, one that requires users to first install the ZeroNet software and the other which allows users direct access to the Amaq Agency’s site without downloading the software. Al Battar advised that this was an experimental project and requested that their followers provide feedback through their Telegram Bot. The post from Al Battar promoting ZeroNet has been shared on several Arabic-language pro-ISIS Telegram Channels.

A review of the Amaq Agency’s ZeroNet website shows that they began testing the platform three weeks ago, shortly after their testing of the Rocket.Chat platform. At this time, Nashir News Agency has not indicated their use of the ZeroNet platform, but it is likely that they will create a ZeroNet website as well.

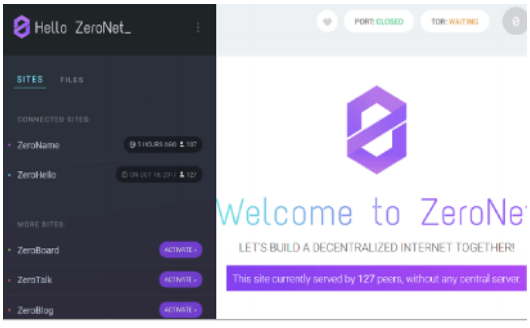
There have been previous attempts by pro-ISIS organizations to use ZeroNet. At that time, ISIS supporters expressed their frustration at failed attempts to download the software and it did not appear to get widely utilized.

- In September 2016, members of the pro-ISIS Cyber Kahilafah promoted their ZeroNet website on their Telegram Channel. They used their ZeroNet channel to post manuals and guidance for lone wolves.

- On 19 August 2016, the pro-ISIS Ansar Al-Khilafah Media announced that they had created an uncensorable backup for their WordPress website on ZeroNet. Ansar Al-Khilafah described ZeroNet as a "secure and decentralized network which uses crowd-sourcing and BitTorrent technology to host websites." Ansar al-Khilafah explained that "this means the website cannot be deleted as it hosted by everyone who visits it, and the people who visit it automatically download it and start seeding the website to new views".

What is ZeroNet?

ZeroNet is a free, decentralized peer-to-peer (P2P) network that distributes content directly to its users without needing a central server. Both open-source and uncensored, ZeroNet is accessible by whomever, whenever, and requires no configuration prior to operation. It supports all modern search browsers and operating systems, giving its users real-time updated content, regardless of connection speed. Additionally, users have the capability to continue browsing sites even without internet connection. Because this network is so far-reaching, ZeroNet is extremely difficult to shut down. As long as there is at least one person using the platform, site failure is close to impossible.



ZeroNet hosts websites utilizing Bitcoin cryptography and the BitTorrent network. Such cryptography, specifically Namecoin cryptocurrency, supports the network's decentralized .bit domains. User accounts are protected by the same cryptography found within a Bitcoin wallet, eliminating the need for passwords. Rather than having an IP address, every site is identifiable by their public key (a bitcoin address) and can only be modified by their creator's private key. Every downloaded file from a ZeroNet public key is verifiably safe and free of any malicious code insertions or modifications. According to the ZeroNet site, it would take a supposed 1 billion years for the world's current supercomputer to "hack" into a private key.

When visiting a ZeroNet site, the user's IP address is requested from BitTorrent trackers, subsequently registering their IP address as a visitor. Sites are served as soon as a user visits them, however, if a user wants to keep their IP address anonymous, they may do so by utilizing the Tor network. On ZeroNet, users also have the option to engage in multi-user sites in which users can request permission from a site owner to post on their site. The site owner only needs to create a new file and set their authorization address as the valid signer. Once this is published, a user's permissions as a previous visitor will have changed. Other features of ZeroNet include one-click site cloning, no backend code, and instant content distribution.

Outlook and Implications
In spite of the persistent suspension of their accounts across various platforms, social media continues to be an effective tool used by ISIS and their supporters. The CFIX assesses that understanding the methodology used by pro-ISIS media accounts during the initial testing of alternative social media platforms could provide law enforcement the ability to identify potential platforms of interest prior to ISIS establishing a significant presence. In particular, identifying Amaq Agency and/or Nashir News Agency accounts on alternative platforms could indicate that platform is favored by ISIS and their supporters.

Cyber Criminals Likely Obfuscate Exploitation through Web Browser Extensions, Increasing Ability to Distribute Malware to End Users

The FBI assesses cyber criminals likely use web browser extensions (WBE) as an intrusion vector, allowing for distribution of malware to end users.

The FBI assesses cyber criminals likely use WBEs as intrusion vectors, allowing for distribution of malware to end users. WBEs allow control of network connections and interface with the victims' web browser use, and malicious WBEs perform functions such as forcing the victim computer to connect to a botnet, stealing a victims' sensitive login credentials, and modifying what the victim sees on a website.

- On 04 September 2018, according to a technology website with indirect access, cyber criminals hacked into a WBE developer's account and released a maliciously modified version of the WBE into a popular Internet browser web store. The modified version included malicious code that would steal usernames, passwords, and private keys for cryptocurrency trades. The malicious WBE also requested elevated privileges that would enable the cyber criminal to read or change all website data viewed by the victim.
- On 09 July 2018, according to a technology website with indirect access, cyber criminals took over a virtual private network (VPN) WBE developer's account to push a malicious version to a popular Internet browser web store. The malicious version of the WBE would redirect users intending to visit a specific cryptocurrency website to a

phishing site designed to steal a victim's credentials, providing cyber criminals access to the victim's funds.

- On 06 July 2018, according to FBI forensic analysis with direct access, a cyber criminal compromised a computer via a malicious VPN WBE that made outbound connections to an Internet protocol address tied to a known botnet.
- On 02 August 2017, according to a technology website with indirect access, cyber criminals hacked a WBE with more than 1 million users through a spear phishing email targeting the WBE developer. The cyber criminals added malicious code for ad injection into the victim's browsers and enabled malicious Javascript execution.
- From June to August 2017, according to a technology website with indirect access, cyber criminals engaged in a spear phishing campaign targeting WBE developers. Spear phishing emails, purportedly from a popular Internet browser company, informed the developers their WBE in the web store was broken and needed an update. The email included a web link to a malicious copy of the Internet browser company's developer website, designed to steal credentials.

Perspective

WBEs assist in improving a web browser's user interface, security, or accessibility for easier Internet browsing. Popular WBEs allow for blocking of intrusive pop-ups, blocking advertisements, storing sensitive website credentials, and customizing the web browser's user interface. Cyber criminals increasingly select WBEs as an intrusion vector because of the trust a victim places in them and the WBEs' ability to auto-update, pushing malicious code to the victim without notification. By hacking WBE developer accounts, the cyber criminal exploits many victims with the WBE already installed, removing the social engineering required to convince a victim to download the WBE. Many times, a cyber criminal will obfuscate the malicious WBE as something beneficial to the victim, such as a VPN tool, which normally would have outbound connections and does not raise an alarm when monitored by a victim.

This intelligence bulletin reflects the FBI's first assessment of the execution of malicious code via WBEs.

Analysis of Alternatives

The FBI considered the alternative hypothesis that in some cases the WBE developer likely was targeted by another WBE competitor in an act of sabotage to diminish the reputation of a WBE. The FBI deemed this alternative less likely because it would decrease trust in the same popular Internet browser web store from which the competing WBE developer benefits. If the FBI or open sources observe indications of WBE developers partaking in malicious WBE takeovers, such as spear phishing emails originating from known WBE developer email accounts, the FBI will reevaluate this hypothesis and increase the level of likelihood.

Outlook

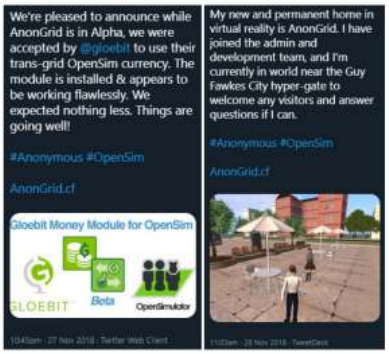
The FBI assesses in the near term cyber criminals likely will increase their targeting of developers of popular WBEs through spear phishing, and less sophisticated cyber criminals will flood the popular Internet browser web store with malware designed to lure victims by masquerading as legitimate WBEs. Victims' innate trust of WBEs hosted on the Internet browser web store increases cyber criminals' illicit financial gain and decreases the integrity of victim computers because of the cyber criminals' ability to modify the computer system. Indicators of this assessment are increases in victim complaints of malicious computer use after installing a WBE or increased cyber criminal discussion about WBE targeting or development within underground forums and marketplaces.

Source: FBI

Anonymous-Related Individuals Create Virtual World for Online Communication and Commerce

A series of social media accounts who claim to be related to and in support of the Anonymous collective have shared images, links, and information regarding a new virtual universe, AnonGrid. AnonGrid is an Open Simulator (OpenSim) virtual world that uses avatars (an online representation of the user) to facilitate conversation and business transactions. AnonGrid is one of many worlds within the Metaverse, which is described as a shared virtual space. These virtually enhanced worlds are popular locations for online interactions and communication, with one of the most well known being "Second Life." According to the AnonGrid creators, AnonGrid is an "OpenSim hyper-gate enabled world in the Metaverse for those interested in or affiliated with the Global Collective of Anonymous."

The first social media post regarding AnonGrid was shared in late November 2018, and in that time additional information has been shared via various sources. Posts cover topics such as the purpose of AnonGrid, updates on the status, as well the capabilities and purpose of the AnonGrid virtual world. The AnonGrid virtual world is said to include:

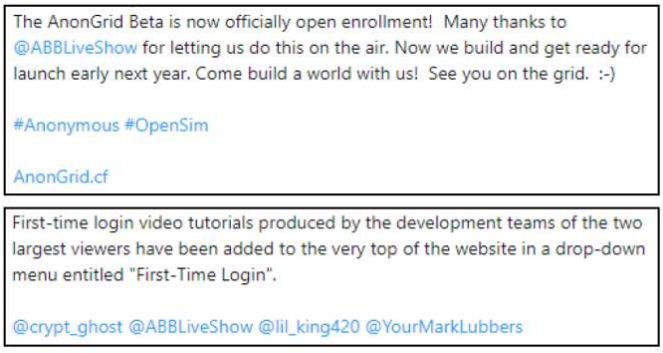


- **Virtual Land:** Each AnonGrid user account is eligible to receive a free parcel of 'land' which is to be used for 'residential purposes.' According to the creators, users who would like a public space for meetings are also able to utilize free private and public virtual properties that can be used for organizations, projects, or coordinating online operations. Moreover, additional properties are available for rent or sale.
- **In-World Purchases:** Merchants are able to sell goods and services within the capital of the AnonGrid

world, Guy Fawkes City. These purchases are paid for exclusively with GloeBit, a transgrid virtual currency, which is used in multiple virtual worlds.

- **Audio Communications:** According to a post from the main Twitter account that shares AnonGrid updates, they have paired with Vivox voice services to employ two-way audio communication among users.
- **Troubleshooting and In-world Guidance:** In-world questions or purchases can be completed with “Wifi Admin” avatars, while problems can be addressed via email outside of the AnonGrid world. Additionally, the AnonGrid administrators are available for new user questions and to “welcome visitors”.

Despite the multiple social media posts regarding the capabilities and advancements that are seen in the AnonGrid world, the creators have also experienced some setbacks in terms of development. On 02 December 2018, the main account associated with updates stated that the “grid suffered catastrophic cascade failure” and user data was lost. Regardless of this, the creators have stated that the AnonGrid world is currently back online, and have since begun enrolling new users. Also, in previous posts, the creators have stated that the AnonGrid virtual world will remain live during any system malfunctions, as they have only just completed the beta testing portion of development. In response to additional bugs that are expected to occur as well as user concerns, the social media account which shares most of the AnonGrid updates has begun sharing video tutorials and states any system glitches should be worked out as enrollment continues.



Outlook and Implications

Due to certain AnonGrid capabilities which have been highlighted by these social media sites, specifically free meeting spaces for operation planning, there is a possibility that the AnonGrid virtual world may be used to coordinate hacking campaigns or cyber-attacks under the pretext of the Anonymous movement. Additionally, because virtual spaces can be purchased using legal tender or cryptocurrencies, the possibility for financial crimes to be perpetrated online also exists. While much of the information regarding the AnonGrid virtual platform is speculative at this point, should this become popular with hackers and cybercriminals, the ability to speak without restriction or buy and sell goods, may become a concern for law enforcement and cyber professionals in the future.

DC Schools Launch New Panic Button App to Alert First Responders in Crisis Situations

DC Mayor Muriel Bowser says this new tool could potentially save your child's life if they were involved in a school shooting situation. The new app called the 'Rave Panic Alert Button' will provide all of the necessary information - about who we are, where we are, and the building we are in - instantly and give first responders vital information when responding to an urgent crisis, like an active shooter. “The additional information contained within a facility profile, provides our officers both on a school campus or anywhere in the district with critical information that allows them to handle whatever situation they are faced with as efficiently as possible,” said Metropolitan Police Department Commander Michael Coligan. Every school in the District and every DC building now has this app and can use it for any of these emergencies. In schools, teachers and administrators could alert police to an active shooter situation, and the app instantly tells first responders where the school is and offers blueprints of the building. First responders will know where to enter and how to maneuver the building before they get there. The Mayor's Office says the app will be rolled out in all DC schools and government buildings immediately.

Source: WJLA - Author: Drew Wilder

Homeland Security Program to Work on Correcting the Vulnerabilities with GPS

The Department of Homeland Security’s Science and Technology Directorate (S&T) recently launched a multiyear program dedicated to finding solutions to global positioning systems’ (GPS) vulnerabilities in critical infrastructure. The program will conduct vulnerability and impact assessments, explore complementary timing technologies, engage with industry through outreach meetings and events, and develop mitigations. S&T already is working to develop cost effective mitigation technologies for GPS interference. Mitigation technologies include the Total Horizon Nuller antenna, which was developed with the Homeland Security Systems Engineering and Development Institute.

Source: Homeland Preparedness News - Author: Melina Druga

Ryuk Ransomware Affects Systems at US Industrial Supply Company

Scope. This Intelligence Note provides recent information and technical indicators from a ransomware attack by unknown cyber actors. CYMC prepared this Note for private sector network defenders. The information cutoff date for this Note is 26 November 2018.
Unknown cyber actors on 8 November 2018 compromised the network of a known US industrial equipment supply company with Ryuk ransomware, according to an FBI report derived from a call-in claiming direct access to the information. The compromise shut

down the company's data backup and recovery systems, as well as at least five other systems on the network. All infected systems were running the Windows operating system, according to the same report.

Ryuk Ransomware

Ryuk is a ransomware that encrypts files on the host computer, stops numerous services, and halts a variety of processes that may interfere with its ransomware functionality, most of which are related to antivirus, database, and back-up software, according to a US cybersecurity firm with expertise in malware analysis.

Support to Computer Network Defense

Ryuk ransomware executable files followed a similar naming convention of five repeated alphabetical characters, terminated with an ".exe" file extension, according to the same report.

The file named FFFFF.exe was stored in the "C:\Users\Public" folder. This file modified the system's startup procedures, which enabled persistent access to the compromised system, according to the same report.

File names and associated MD5 hashes (see below)

File Name	MD5 Hash
BBBBB.exe	26684125fb9ad32668e07dcb8e3f1c5d
CCCCC.exe	
FFFFF.exe	
155.exe	N/A

Source: DHS

North Korea-Linked Hackers Target Academic Institutions

A threat group possibly originating from North Korea has been targeting academic institutions since at least May of this year, NetScout's security researchers reveal.The attackers use spear-phishing emails that link to a website where a lure document attempts to trick users into installing a malicious Google Chrome extension. Following initial compromise, off-the-shelf tools are used to ensure persistence.

The campaign likely hit other targets as well, though NetScout says that only those domains targeting academia were intended to install a malicious Chrome extension.

Many of the intended victims, across multiple universities, had expertise in biomedical engineering. The campaign, which NetScout refers to as STOLEN PENCIL, employed many basic phishing pages, the researchers say. The more sophisticated phishing pages that targeted academia displayed a benign PDF in an IFRAME and redirected users to a “Font Manager” extension from the Chrome Web Store.The extension loads JavaScript from a separate site, but the content of the file was found to contain legitimate jQuery code, likely because the attacker replaced the malicious code to hinder analysis. The malicious extension would read data from all of the accessed websites, suggesting that the attackers were looking to steal browser cookies and passwords.

Source: Security Week

B&Q Data Leak Exposes Information On 70,000 Thefts From Its Stores, Including Names of Suspected Offenders

Internal database was accessible to the world - no password required.

If you run a chain of superstores up and down the UK you have to recognise that from time-to-time ne’er-do-wells are likely to steal goods from your shelves.

And so it wouldn’t be a surprise if those stores maintain a database of the names of those people who they have caught stealing products, what was stolen, the value of the good stolen, and which stores they were stolen from.

After all, you might wish to ban people who have stolen from you in the past, or suspect might steal from you in the future, from your premises.
Oh, and one thing is for sure - you certainly would want to make sure that such a database wasn’t itself easy to steal…

Unfortunately, according to security specialists at Ctrlbox, well-known UK household goods and hardware store B&Q has been careless with its database for tracking offenders and thefts - leaving it wide open for anyone on the internet to access.

A database of 70,000 offender and incident logs was only supposed to be accessible internally within B&Q, but was instead exposed for anyone to access.
The offending (ho ho..) data was on an ElasticSearch server - a technology used for powering search functions - and was not protected by a password.

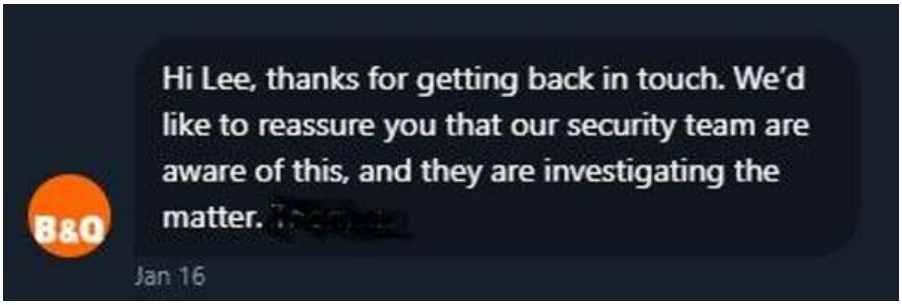
The nature of the data (alleging possible criminal activity and including in some cases people’s names and vehicle details) meant, of course, that it could be considered highly sensitive and could have serious repercussions if it fell into the wrong hands through such sloppiness.

```
▼ description:    "Offender ran out of the fire
                  exit with nest thermostats.The
                  male on this occasion got
                  away.there is no CCTV footage
                  covering this area.\r\n\r\nno
                  CCTV coverage of the theft or
                  witnesses"
```

That's obviously bad. But what makes things worse is the hoops Ctrlbox had to jump through in order to get the data removed from the internet.

Having determined that the breach was related to B&Q by analysing GEOIP information, product codes, and types of goods listed in the exposed data, Ctrlbox's Lee Johnstone sent a notification to the store's support team. This was followed a day later by a message to B&Q over Twitter.

Four days after the first notification, Johnstone says that the data was still wide open: "…clearly they had not got the message and it was becoming clear that B&Q was not going to act on this any time soon, so another message was sent to support who once again assured me that the message had been sent to the right people."



Johnstone says that after a week he had communicated with three different support staff, but nothing had been done. He even tried messaging B&Q CEO Christian Mazauric on LinkedIn (according to Johnstone, Mazauric read the message, but never replied).

The offending ElasticSearch server only finally went offline two days ago - almost two weeks after B&Q was informed about the problem.

Companies need to act more quickly when informed of serious security breaches. And all staff, even if they don't have the ability to assess the seriousness of a security issue themselves, need to understand the importance of escalating it to the right team in a prompt fashion.

Source: Graham Culey

Global Hacking Campaign Takes Aim at Finance, Defense, and Energy Companies

A global hacking operation is targeting government departments, defense, telecoms, and other high-tech organizations around the world in what appears to be the first stage of a cyber espionage campaign. Sharpshooter

Dubbed Operation Sharpshooter by researchers at McAfee, the new campaign has only been active for a matter of weeks, but hit 87 organizations in 24 countries during October and November alone, with the aim of the operation seemingly being intelligence gathering. While organizations across the globe have been targeted by the campaign, analysis by McAfee suggests that victims are predominantly in the US.

The main focus of the attackers appears to be defense and government departments but businesses in the telecommunications, energy, nuclear, and financial sectors have also been targeted in the espionage campaign. Researchers note the attacks display many of the hallmarks of the Lazarus Group, a hacking group working on behalf of the interests of North Korea - but say that alone is not enough to confirm attribution.

The operation began on 25 October, with a series of phishing emails masquerading as recruitment emails sent to a number of targets. All of the malicious Word documents share the author name - Richard - and contain job descriptions for positions at various companies. The documents contain a malicious macro that leverages embedded shellcode to inject a downloader for the Sharpshooter malware into the memory of Word. This then serves as a downloader for the second stage of the campaign: implanting

Rising Sun.

Rising Sun Rising Sun is a modular backdoor that performs reconnaissance on the victim’s network, providing the attackers with access to machine-level information including documents, usernames, network configuration, and system settings, information about which is sent to a command and control server. The malware can also execute various commands, get additional files, and is capable of clearing memory and deleting activity.
Analysis of Rising Sun suggests that it shares code and configuration data with Duuzer, a family of trojan malware used in the Sony hack - an incident which the United States holds North Korea responsible for. However, the decryption scheme of Rising Sun is different, suggesting it could potentially be an evolution of Duuzer. If it is, it would not be the first example of North Korean hackers re-using old code to build new attacks - as McAfee has previously noted.

Source: ZDNet

Fighting Deepfakes Will Require More than Technology

Deepfakes—fake but incredibly realistic photos, videos, or audio created with machine learning—are receiving increased attention in the national security arena due to their ability to manipulate or deceive. Pervasive among discussions of countering deepfake technology is how machine learning can be used to detect fraudulent content made with these systems (here, here, here, and here, for instance). Machine learning is an important countermeasure, but the idea that "good" technology is necessarily the best and only needed solution to "bad" technology is fantasy.

To counter the threats posed by this emerging technology, strategies must be broad, nationally coordinated, and entail solutions that are technical, human-focused, and societal-focused writ large. There is perhaps no better demonstration of this idea than the evolution of how government, industry, and individuals respond to cyberattacks

Despite these lessons from countering cybersecurity threats, the same fallacy—that technology will be enough—is all too prevalent in discussions of countering the potentially harmful effects of deepfake photo, video, and audio. It makes sense in context: Social media giants largely left the identification of fake news up to end users. That changed, suddenly, when end users realized they were being manipulated in order to make money or distort public discourse and manipulate election results. In response, online platforms ramped up their technical efforts, building algorithms to "contextualize" news with other sources on the issue. They changed their rules around fake accounts and disinformation. They hired more staff to deal with the issue. Again, bad press, user dissatisfaction, and government pressure played a role in these changes.

Source: NextGov

Apple Launches New Transparency Report Website Showing Government Data Requests from around the World

In recent years, technology companies have been under increasing pressure to be more transparent about the requests for data they receive from global governments. Firms such as Microsoft, Google, and Facebook publish regular transparency reports, and Apple is no different. Now the company has launched a new transparency report website which makes it even easier to trawl through its twice-yearly publication and see how many data requests have been issued by different governments. While previous reports have been hard-to-browse documents that were a pain to sift through, the new site makes it easy to home in on data and easier to make comparisons between countries. A simple pair of drop-down menus makes it possible to specify a range of dates and a country you want to know about, and you'll be furnished with figures about the number of "device", "financial identifier", "account" and "emergency" data requests have been received. It is still possible to click through and see a traditional, static report for individual countries, but the new interactive elements make all of the data much easier to navigate. One can browse through the figures and be able to see that there has been something of an increase in government requests for data - up some nine

percent since the last transparency report. Note: There is a limit to just what Apple reveals in the reports. See the full report on Apple's new transparency report website.

Source: betanews

Analyst Comment: The Transparency Report shows Apple received a total of 32,342 requests from 84 different governments around the world to access 163,823 devices between January and June of 2018. Of those, 4,570 requests were from the US, and data was provided 81% of the time. Device requests seek information associated with devices such as the Apple serial number and are generally made for law enforcement investigations.

Microsoft's Search Engine Bing Shows Child Pornography, Report Finds

Microsoft's Bing is allowing child pornography images to appear in its results and is aiding pedophiles by suggesting other terms they could search for. An investigation by AntiToxin, an online safety company, found multiple cases of the illegal images showing up in the search engine's results.

The search engine had the illegal images in results when terms such as "porn kids" or "nude family kids" were typed into Bing, according to the TechCrunch website. The site's search suggestions also directed the researchers to child pornography. For example, the term "Omegle Kids", referring to a video chat app that is popular with children, suggested the search "Omegle Kids Girls 13" which produced illegal imagery. Another search for "Omegle for 12 year old" prompted Bing to suggest searching for "Kids On Omegle Showing" which led to illegal images.

Bing would also show users additional explicit pictures of children through its "similar images" feature. Searching for child pornography online is illegal and the investigation took place under the close supervision of lawyers and authorities, Techcrunch said. Bing says it has removed the images and promised to make changes to how users can report what it calls problematic images and video content. Microsoft called the search results "unacceptable" and said it had immediately removed them once they had been reported. The company has claimed to be at the forefront of the fight against online child abuse by using a technology called PhotoDNA, which automatically blocks illegal images from being uploaded.

Andy Burrows, the NSPCC's associate head of child safety online, said: "It is shocking that as law enforcement agencies are working hard to stop child abuse images being shared online, these images are readily appearing in Bing search results, with the search engine's algorithms even recommending more. "The NSPCC's Wild West Web campaign has been calling on government to create an independent regulator to force tech companies to protect children and stop such material being shared, and to make them accountable when they fail to do so."

Source: The Telegraph - Authors: Olivia Feld and Mike Wright

Amazon Sent 1,700 Audio Recordings of Alexa User to a Stranger

An Amazon customer in Germany under the European Union data protection law called GDPR (General Data Protection Regulation) requested the company to send all the data it stored on him but little did he know he was about to get his hands on a trove of 1,700 audio recordings of a stranger speaking in their home.

The unidentified customer told c't, a German technology website, that he had never used any of Amazon's voice activated assistants and recordings belonged to a customer having a private conversation in his home. "I was very surprised about that because I don't use Amazon Alexa, let alone have an Alexa-enabled device," the customer told the magazine. "So I randomly listened to some of these audio files and could not recognize any of the voices." According to the magazine who heard the content of audio recordings confirmed that it included a man's voice from inside his home while some of the recordings also had a female voice, sounds of alarm clocks and conversations about family's private life and work. The customer then reported the incident to Amazon but did not receive any response, yet audio files were later deleted from the link that was provided by Amazon, Reuters reported. However, it was too late since the customer had already downloaded all the files on their system.

Amazon, on the other hand, acknowledged the privacy breach and said that it was an "isolated incident" and "an unfortunate case that resulted from a human error." The company issued a statement saying that it "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." Additionally, in May this year, Amazon Echo sent a couple's conversation recordings to the husband's employee. In the most recent incident, Amazon also exposed names and email addresses of its customers on its website.

Source: HackRead

Analyst Comment: Users of IoT devices must remain vigilant; Alexa devices (for example) continue to listen for commands for 60 minutes after receiving instructions, meaning any conversation heard by one of these devices might be recorded. Users might consider using the mute button on this and similar devices when not issuing commands. Government organizations should take steps to assure that these devices are not present in their environments, as they present a security risk on networks. Even when placed on public wireless, IoT devices present a risk to conversations that may be private without agreements and may leak not public organization conversations without consent and vetting.

Russian Influence Actors Attempted to Amplify "Yellow Vest" Protest, Spread of Movement to US States

Scope. This Intelligence Note provides state and local stakeholders situational awareness related to ongoing Russian influence activity in the United States regarding the "Yellow Vest" protest movement that originated in France and has gained support from at least one US group that planned to protest at an event in California.a Russian influence actors continue to amplify divisive narratives, such as the "Yellow Vest" movement, in the United States and the West. Further, variants of these titles or related topics in this Note, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. Consider this information in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties. This Note is written in direct support of the DHS Countering Foreign Influence Task Force. The information cutoff date for this Note is 04 January 2019.

Russian-Linked News Website Promotes Narratives about US Group Planning to Use "Yellow Vest" Movement to Protest California Governor Inauguration

A Russian-linked news website on 30 December 2018 published an article describing a US-based group that plans to protest the California Governor's inauguration on 07 January 2019, according to a DHS open source intelligence report.1,b The group wears yellow vests in support of the "Yellow Vest" protests in France, according to a news article.2 We have not seen any reporting suggesting the protests will be violent or that the protests are instigated or coordinated by Russian influence actors.

Ongoing Russian Influence Activity Related to "Yellow Vest" Movement

- Russian influence actors—using Twitter accounts suspected of being controlled by Russian influence actors, Russian state media, and a Russian-linked news website—have published articles and promoted content since mid-November 2018 about the "Yellow Vest" or "Gilet Jaune" movement that began in France to protest against a proposed fuel tax, according to open source posts from publicly available accounts and an information security company.3,4

- The Russian-linked news website that promotes misinformation through articles and podcasts published an article encouraging Americans to support the "Yellow Vest" protests in mid-December 2018, according to a DHS open source intelligence report.5 During the 2018 US Congressional election cycle, the website created and maintained an "Elections" tab dedicated to news about congressional campaigns and candidates; articles often promoted narratives of voter fraud, abuse of power, government and social media censorship, and challenges voters faced on Election Day, according to open source posts from publicly available accounts.6

- Twitter accounts, some of which are suspected of being controlled by the Internet Research Agency and other Russian influence actors such as state-controlled media outlets, have posted and re-posted content from other users that support the "Yellow Vest" protestors and criticize the French Government's response, according to a US-

based private sector entity that analyzes the activity of social-media accounts linked to Russian influence operations.7 Particularly, such accounts have amplified content critical of French President Macron—using hashtags including #MacronMustGo and #MacronDemission—and alleged police brutality against protestors and censorship of the movement by mainstream media. Additionally, these accounts have mocked the idea that Russian influence actors are conducting influence activity related to the movement, according to the same private sector entity.

- One account suspected of being controlled by Russian influence actors from early December 2018 to early January 2019 shared Russian state media articles and retweeted other users who post about “spinoff” protests in Israel, Spain, Germany, Italy, the UK, and Canada, according to data and content from publicly available social media accounts.8

- One account suspected of being controlled by Russian influence actors from early December 2018 to early January 2019 shared Russian state media articles and retweeted other users who post about “spinoff” protests in Israel, Spain, Germany, Italy, the UK, and Canada, according to data and content from publicly available social media accounts.8

- Russian state media outlets have focused primarily on the protests in France—though at least one article described a related protest in the UK—emphasizing narratives about calls for French President Emmanuel Macron to resign and police brutality against protesters, according to a known Russian Government-linked media outlet. 9,10,11,12 Other articles challenged news media outlets’ stories about alleged Russian interference related to the protests.13

Source: DHS

Hackers Target Organizations in the Naval and Maritime Sectors

Companies and infrastructure within the naval and maritime sectors are under attack. In recent years, security experts have observed a growing number of attacks carried out by different types of attackers, including cybercrime syndicates and nation-state actors. On the morning of 20 September 2018, the Port of Barcelona was hit by a cyber-attack that forced the operators of the port’s infrastructure to launch emergency procedures. A few days later, several computers at the Port of San Diego were infected with ransomware. The incident impacted the processing of park permits and record requests, as well as other operations.

The incidents have raised discussion about security for these types of critical infrastructures and demonstrated that ports and other such locations are too vulnerable to cyber-attacks. The increased usage of computer systems for navigation, container inspection, design, and manufacturing of vessels is exposing the industry to cyber-threats. The design center, ships, and safe navigation, satellite communications systems, tracking systems, marine radar systems, and automatic identification systems

are just a few examples of potential targets for attackers. According to experts, the rapid and increasing convergence of IT and OT systems, along with the diffusion of connected devices, is exposing the navy and shipping to cyber-threats. Threat actors could launch cyber-attacks for the purpose of either espionage or sabotage. To mitigate threats, it is necessary to adopt a new model of cybersecurity based on threat intelligence and information sharing on cyber-threats.

The maritime sector is particularly threatened by disruptions due to the role of technology in global trade. Many cyberattacks have been carried out on commercial ships. In one such incident, a commercial ship contracted to the US military was the victim of a cyber-attack powered by suspected Chinese military hackers. In 2012, the China-linked hackers compromised “multiple systems” on a commercial ship on contract to Transcom. Over 2018, the China-linked APT group Leviathan, aka TEMP.Periscope, increased its attacks on engineering and maritime entities. In November the top Australia defense firm Austal, also working with the United States Navy, suffered a serious security breach.

Unfortunately, many cyber-events in the maritime industry have remained undetected. Businesses have also been reluctant to reveal them to the public. Another worrisome aspect is that many organizations in the maritime industry are not properly conducting regular security assessments to evaluate their vulnerability to a cyber-attack.

Source: Infosec - Author: Pierluigi Paganini

Potential Use of ‘Mastodon Social’ as Twitter Alternative

This bulletin was created by the Central Florida Intelligence Exchange (CFIX) to provide background on a lesser known social media platform, Mastodon Social, and its potential use an alternative to Twitter. This information is intended to support local, state, and federal government agencies along with the private sector in developing/ prioritizing protective and support measures relating to existing or emerging threats to homeland security.

First Amendment Acknowledgement
The CFIX recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The CFIX safeguards these rights and reports on only those activities where the potential use of rhetoric and/or propaganda could be used to incite individuals to carry out acts of violence. Additionally, potential criminality exhibited by certain members of a group does not negate the constitutional rights of the group itself or its law-abiding participants to exercise their individual liberties under the First Amendment to the US Constitution.

Overview
Mastodon Social is a free, open-source social networking site that extends beyond a singular server and is welcome to whomever wishes to join. Mastodon follows a standard set of protocols that promotes the adoption of newer and greater software as

time progresses so that its users may interact and exchange information with each other as effortlessly as possible. Considered a federation within a website, each independent Mastodon server saves its own data and operates under its own set of rules so that users may publish whatever they want, whenever they want.

Similar to Twitter but community-owned, ad-free, and crowdfunded, Mastodon users are able to chronologically browse their feeds without interruptions, viewing only the material they want to see. Mastodon's platform makes it harder for larger corporations to collect information, track data, enforce rules, block accesses, and shut down servers.

Recognized for its decentralized structure and subsequent diverse audiences, Mastodon Social has acquired the potential to be utilized as a Twitter alternative by violent extremists. White Supremacy Extremists have discussed using Mastodon on Gab while Anarchist Extremists have been seen promoting the site on their Twitter profiles and blogs. Another interesting find was discovering that an Australia-made Mastodon server, Switter, has become home to many sex workers as they run out of safe online spaces. Since its launch in March 2018, Switter has grown to be the sixth largest server on Mastodon.

What is Mastodon Social?

According to their website, Mastodon Social is an easy to access social network of various independent communities. To join, users download the free Mastodon software from the internet and then select a server that caters to their interests (or they can make their own). Anyone can create their own server, uniquely known as an "instance," in which creators can then run, moderate, and institute their own code of conduct. Within each instance is a community of individuals that share a similar set of values and beliefs, allowing the user to comfortably navigate through posts they approve of. Instances can communicate with other instances but only if they allow it. If controversial content arises, each server has their own administrators and may even employ a moderation team. Moderation teams, along with anti-abuse tools, help to ensure that Mastodon users are protected from the material they do not want to see.

Like Twitter, Mastodon users can post pictures, videos, messages (within the 500-character limit), and follow other profiles. Users can hide posts behind "sensitive content" warnings and edit what they have already posted. However, unlike Twitter and in an effort to prevent unwarranted fighting, users cannot search for random keywords nor can they quote another post on Mastodon. Furthermore, users can select who can view each individual post. Posts can be made fully public meaning it is visible to a user's followers, public timelines, and anyone else viewing that person's profile. A post is considered unlisted when it is left out of the public timelines. A post can also be private when it only appears to a user's followers and the people mentioned in it. A post can be direct which means it is only visible to those users who are mentioned in it. Hashtags are the only part of a post that is searchable within Mastodon.

Mastodon is available on multiple free and paid apps for both iOS, Android and other platforms. These apps include Tusky, Subway Tooter, Mastalab, Toot! Mast, Amaroq, Pinafore, Tootle, and Tooter.

Hackers are Spreading Islamic State Propaganda by Hijacking Dormant Twitter Accounts

Hackers are using a decade-old flaw to target and hijack dormant Twitter accounts to spread terrorist propaganda. Many of the affected Twitter accounts appeared to be hijacked in recent days or weeks, some longer, after years of inactivity. A sudden shift in tone or the language used in tweets often gives away the hijack, usually a single tweet in Arabic, sometimes praising Allah or retweeting propaganda from another account.

Twitter has suspended most of the accounts reviewed, but some remain active. The recent resurgence in hijacked accounts appears to be hackers exploiting Twitter's legacy lack of email confirmation. Twitter took steps to prevent the automated creation of new accounts in June by requiring new accounts to be confirmed using an email address or phone number, but many older accounts remain unconfirmed.

However, while dormant Twitter accounts are never deleted, the email addresses that were used to create them either never existed in the first place, or expired long ago. As such, many older Twitter accounts can be easily hijacked by creating the email address used to initially register the Twitter account.

"This issue has been around for a while but no one really knew and took advantage of it," said a hacker and security researcher known as WauchulaGhost, who researches and disrupts the online activities of the so-called Islamic State. "Now, we have Islamic State supporters that have figured it out," he said.

He found one since-suspended account following many inactive accounts, which had all been recently hijacked. His hypothesis was that, "once you create the email, password reset on the Twitter account, check the email and click the link," he said. Many of those dormant accounts he tested had not created the email that the account was registered to. The email addresses are partially masked, but its easy to tell how many characters are in a Twitter account's email address. Often the email accounts were simply their Twitter handle at "@hotmail.com" or "@yahoo.com," he said. Some of the accounts had tens of thousands of followers, he said.

He shared several of those dormant Twitter accounts with TechCrunch, nearly all of which had registered email addresses that were identical to their Twitter handle. He was able to register all of those email addresses, which would have allowed him to access those accounts.

Many of the hijacked accounts found were spreading propaganda, but were later suspended from the service. The hackers often did not change the bios on the account. The hijacked accounts we reviewed included Arabic-speaking videos of Islamic State fighters wielding weapons and other curated content. Others simply contained text, also in Arabic, that praised violence and other attacks, or retweeted other accounts. One tweet, roughly translated, used an Islamic State hashtag: "…with your cars, let's go pack, you bomb, go with a bomb, you go in any way." Another hijacked account called on Muslims to "kill these Christians wherever you find them," while another account tweeted about turning the Christmas holidays "into grief and horror." (These statements go against fundamental Islamic teachings, and calls for violence against non-Muslims is expressly forbidden in the Qur'an.)

Twitter said it is trying to find a solution to a problem that it claims is not theirs to fix. "Reusing email addresses in this manner is not a new issue for Twitter or other online services," a Twitter spokesperson told TechCrunch. "For our part, our teams are aware and are working to identify solutions that can help keep Twitter accounts safe and secure."

In other words, it is the email providers, like Hotmail and Yahoo, that are deactivating accounts and recycling email addresses that are partly the problem, on top of Twitter's lack of confirming accounts for the first decade of the service's existence. Twitter is not alone: Facebook also struggled with account hijacks through expired email accounts.

Twitter said it has removed over a million accounts for promoting and sharing content since August 2015 — with more than 205,000 accounts during the first half of 2018 alone. The number of accounts suspended has declined in each reporting period as Twitter claims its technologies are preventing pro-terrorism accounts from spreading content in the first place. Even during the reporting for this story, we've even seen account after account get suspended off the site by Twitter. Around one-quarter of accounts that are eventually caught are still able to tweet at least once, it says. Twitter knows it has a problem. With other companies as much at fault, neither they, nor the social media giant, appears to have a way to fix it.

Source: TechCrunch

Forget Bitcoin Why Criminals Are Using Fortnite to Launder Illicit Funds

With well over 200 million users across the globe, few video games have as large a following as Fortnite. The freemium game is so popular that its developer, Epic Games, banked $3 billion in 2018. However, according to a report on the Independent, Epic Games isn't the only entity getting rich off Fortnite. V-Bucks, the game's official in-game currency, are increasingly being used as a tool for money laundering on the dark web.

How Fortnite V-Bucks are Used to Launder Money

According to researchers, hackers are using stolen credit cards to purchase V-Bucks. From there, the purchased V-Bucks are resold at a discount rate to players, as a means of "cleaning up" the currency. Cyber-security firm Sixgill first discovered these activities. The company's

agents reportedly uncovered the operations by pretending to be potential customers and engaging in transactions with some of the criminals.

Benjamin Preminger, a Senior Intelligence Analyst at Sixgill, said:

Criminals are executing carding fraud and getting money in and out of the Fortnite system with relative impunity.

It is unclear how much money the scammers have been able to make from these operations. However, Sixgill also noted that the amount of money flowing around Fortnite had seen exponential increases as the game continues to grow in popularity.

A Practical Scam for the Dark Web

The scam operation makes much sense. Ever since its release, the online battle royale game has been a massive hit, attracting hundreds of millions of players in the process. The majority of these players are kids and teenagers, who are impressionable and can often easily be scammed.

The dark web, the secluded part of the internet that can only be accessed via specialized software, is where a lot of online criminal activities are conducted. While the money laundering being conducted with Fortnite's V-Bucks can be found on other aspects of the internet (such as social media platforms), these activities are reportedly being carried out on a much larger scale on the dark web.

Are V-Bucks the New Bitcoin?

While it has found increasing use as a store of value and means of exchange in some quarters, Bitcoin has also drawn ire as an alleged tool for criminal activities. According to crypto research firm CipherTrace, criminals laundered over $2.5 billion worth of Bitcoin use from January 2009 to September 2018.

Epic Games, the developer of Fortnite, intends to stamp out V-Buck laundering before it grows to that scale. Speaking with the Hollywood Reporter, a spokesperson for the company said:

Epic Games takes these issues seriously, as chargebacks and fraud put our players and our business at risk. As always, we encourage players to protect their accounts by turning on two-factor authentication, not re-using passwords and using strong passwords, and not sharing account information with others.

The 'Milly Rock' Lawsuit

This new report is only the latest in a growing list of struggles for Fortnite and its producer. In addition to the money laundering claims, Epic Games is also facing a lawsuit from rapper 2 Milly over the developers' misappropriation of the "Milly Rock" dance. The lawsuit was filed last month. The dance, which was featured back in 2014 in a video for "Milly Rock" (a song, which bears the same name as the dance), was added by Epic Games to Fortnite's fifth season, albeit under the moniker "Swipe It."

Source: CCN

Decrypted Telegram Bot Chatter Revealed as New Windows Malware

Sometimes it take a small bug in one thing to find something massive elsewhere.

During a recent investigation, security firm Forcepoint Labs said it found a new kind of malware that was found taking instructions from a hacker sending commands over the encrypted messaging app **Telegram** .

The researchers described their newly discovered malware, dubbed GoodSender, as a “fairly simple” Windows-based malware that’s about a year old, which uses Telegram as the method to listen and wait for commands. Once the malware infects its target, it creates a new administrator account and enables a remote desktop — and waits. As soon as the malware infects, it sends the username and randomly generated password to the hacker through Telegram.

It’s not the first time malware has used a commercial product to communicate with malware; hackers are hiding commands in pictures posted to Twitter or in comments left on celebrity Instagram posts.

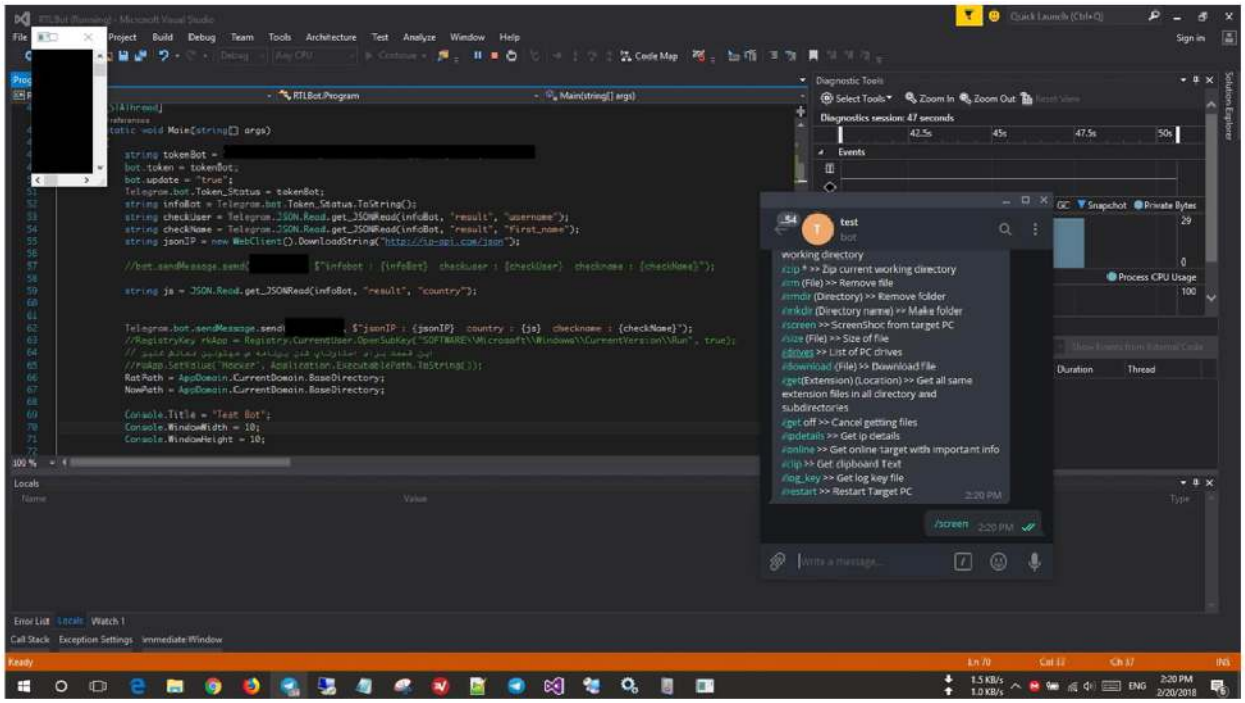
But using an encrypted messenger makes it far harder to detect. At least, that’s the theory.

Forcepoint said in its research out Thursday that it only stumbled on the malware after it found a vulnerability in Telegram’s notoriously bad encryption.

End-to-end messages are encrypted using the app’s proprietary MTProto protocol, long slammed by cryptographers for leaking metadata and having flaws, and likened to “being stabbed in the eye with a fork.” Its bots, however, only use traditional TLS — or HTTPS — to communicate. The leaking metadata makes it easy to man-in-the-middle the connection and abuse the bots’ API to read bot-sent and received messages, but also recover the full messaging history of the target bot, the researchers say.

When the researchers found the hacker using a Telegram bot to communicate with the malware, they dug in to learn more.

Fortunately, they were able to trace back the bot’s entire message history to the malware because each message had a unique message ID that increased incrementally, allowing the researchers to run a simple script to replay and scrape the bot’s conversation history.



The GoodSender malware is active and sends its first victim information (Image: Forcepoint)

“This meant that we could track [the hacker’s] first steps towards creating and deploying the malware all the way through to current campaigns in the form of communications to and from both victims and test machines,” the researchers said.

Your bot uncovered, your malware discovered — what can make it worse for the hacker? The researchers know who they are.
Because the hacker didn’t have a clear separation between their development and production workspaces, the researchers say they could track the malware author because they used their own computer and didn’t mask their IP address.

The researchers could also see exactly what commands the malware would listen to: take screenshots, remove or download files, get IP address data, copy whatever’s in the clipboard and even restart the PC.

But the researchers don’t have all the answers. How did the malware get onto victim computers in the first place? They suspect they used the so-called EternalBlue exploit, a hacking tool designed to target Windows computers, developed by and stolen from the National Security Agency, to gain access to unpatched computers. And they don’t know how many victims there are, except that there likely are more than 120 victims in the U.S., followed by Vietnam, India and Australia.

Forcepoint informed Telegram of the vulnerability. TechCrunch also reached out to Telegram’s founder and chief executive **Pavel Durov** for comment, but didn’t hear back.

If there’s a lesson to learn? Be careful using bots on Telegram — and certainly don’t use Telegram for your malware.

Source: TechCrunch