# OCCAMSEC E-BRIEF // DECEMBER 2018

# Actors Behind SamSam Ransomware Charged and Sanctions Follow

**What is SamSam?**

SamSam ransomware is most famous for the attack that took down the City of Atlanta and has extorted millions from its victims since 2015 and according the US Justice Department 43 states commonly targeting hospitals and infrastructure, .

In a press conference, US Attorney Craig Carpentito told reporters Savandi and Mansouri that attackers worked hard to identify the most vulnerable targets that they could, and not just because they would be more likely to pay up. “Money is not their sole objective,’ he claimed. “They’re seeking to harm our institutions and critical infrastructure, they’re trying to impact our way of life.”

**Sanctions**

For the first time in history, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) has attributed cryptocurrency addressees to individuals involved in the converting ransomware cryptocurrency payments to flat currency.

The cryptocurrency addresses are being attributed to two Iranian-based individuals, Ali Khorashadizadeh and Mohammad Ghorbaniyan.

OFAC has also added these two individuals to the Specially Designated Nationals and Blocked Persons Lists (SDN), which means US individuals and companies are blocked from doing business or conducting any transactions with these individuals. These sanctions could also affect non US businesses and individuals who conduct transactions with them due to secondary sanctions.

**Why is this important?**

If your organization has, as part of its playbook, to pay ransomware demands, this option should probably revisited. In essence, making a ransomware payment could end up causing much larger problems if U.S. sanctions are being violated.

For security firms that have in their arsenal the ability to negotiate and make ransomware payments on behalf of their customers this too needs to be revisited for the same reasons.

**Reference:** Digital Currency Address 149w62rY42aZBox8fGcmqNsXUzSStKeq8C
**Reference**: Digital Currency Address 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V
**Reference**: https://home.treasury.gov/news/press-releases/sm556
**Reference**: UPDATE: OFAC FAQs: Sanctions Compliance
**Reference**: The Verge

**Source**: OccamSec

## Cybersecurity and Infrastructure Security Agency

On 16 November 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

- CISA leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.
- The name CISA brings recognition to the work being done, improving its ability to engage with partners and stakeholders, and recruit top cybersecurity talent.

**What Does CISA Do?**

CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

**Proactive Cyber Protection:**

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal, and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

**Infrastructure Resilience:**

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for US critical infrastructure through the National Risk Management Center.

**Emergency Communications:**

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools, and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.

**Organizational Changes Related to the CISA Act**

The CISA Act establishes three divisions in the new agency: Cybersecurity, Infrastructure Security, and Emergency Communications.

- The Act transfers the Office of Biometrics Identity Management (OBIM) to DHS's Management Directorate. Placement within the DHS Headquarters supports expanded collaboration and ensures OBIM's capabilities are available across the DHS enterprise and the interagency.
- The bill provides the Secretary of Homeland Security the flexibility to determine an alignment of the Federal Protective Service (FPS) that best supports its critical role of protecting federal employees and securing federal facilities across the nation and territories.

**Source**: DHS

## Police Breakthrough Interception and Decryption of Crypto Communication

Police in the Netherlands and the Public Prosecution Service have achieved a breakthrough in the interception and decryption of encrypted communication between criminals. Criminals thought they could safely communicate with socalled crypto phones which used the application Ironchat. Police experts in the east of the Netherlands have succeeded in gaining access to this communication. As a result, the police have been able to watch live the communication between criminals for some time. The server on which the encrypted communication took place was discovered after the police in the east of the Netherlands traced a supplier of the crypto phones in an investigation into money laundering. With these crypto phones, which cost thousands of euros, only text messages can be sent. As a result of using a separate computer server that encrypted the communication, the data traffic became invisible to the authorities.

**Good Information Position**
The operation started after officials received sufficient concrete indications that a man from Lingewaard sold crypto phones to criminals. The police and the Public Prosecution Service take a hard line against people who help criminals by making their activities possible. As a result of the operation, the police and the Public Prosecution Service have taken a good information position. More than 258,000 chat messages have been read, which yields a lot of information. This information can lead to decisive breakthroughs in ongoing investigations. The data can also be used to start new criminal investigations. In this way, evidence has been obtained in on-going investigations and new criminal activities can be stopped.

**Server and Website Offline**
The server and website of the supplier of the crypto phones has now been taken offline. As a result, this important communication channel, with which criminals thought themselves to be unnoticed, belongs to the past. The operation was stopped when criminals were starting to suspect each other of leaking information to the police, which caused safety risks.

**Source**: Politie

## TimpDoor Android Malware Turning Devices into Hidden Proxies

The McAfee Mobile Research team has identified an active phishing campaign that traps users by sending an SMS to influence them on downloading and installing an Android malware app TimpDoor. It is a fake voice-message app that allows attackers to infect the devices and use them as network proxies, without raising suspicion. Once TimpDoor is installed, a Socks proxy service is initiated in the background, which is responsible for redirecting the entire traffic on the network from a third-party server through an encrypted connection facilitated by a secure shell tunnel. This lets attackers get access to internal networks of the system after evading the implemented network security methods, like network monitors, and firewalls. TimpDoor, McAfee researchers say, is malicious .APK that has been presented as a voice application. This app can easily circumvent the security measures by Google's Play Store. However, the attackers are not hosting the Android malware in the app repository but it is being distributed as text messages that contain a link to this app. After invading the system, TimpDoor can convert the infected devices into mobile backdoors in order to compromise home and corporate networks. The campaign has been active since late March, while Android users in the US are the key targets of this campaign. The strange SMS messages inform the recipients that there are two voice messages that they should "review" and to access them, they need to click on an embedded link. Researchers believe that so far this campaign has claimed 5,000 devices in the US. A remote server is used to host the fake app, which is designed to appear genuine.

**Source**: HackRead

**Analyst Comment**: While the attack requires a level of gullibility by the victim, this is a clever approach to gaining access to an otherwise protected network. Organizations should consider using a mobile device management platform to prevent unauthorized software installation. Because mobile devices, especially Android devices, are hard to protect, they should be restricted from connections to internal networks. Finally, organizations should monitor all outbound SSH sessions and should restrict HTTP/HTTPS connections to using web filter/proxy exit nodes.

## DHS Strategy to Protect United States from Electromagnetic Threats

A new Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) was released by the US Department of Homeland Security (DHS) this week. The strategy focuses on DHS efforts to counteract threats to critical infrastructure and respond to them accordingly, be they EMP attacks or naturally-occurring GMD situations. These pose a serious threat to the electrical grid, communications equipment, and transportation capabilities, and the new strategy forms a consensus on how the department can react.

An implementation plan for the strategy is still underway. Once released, DHS will begin evaluating their progress toward plugging capability gaps and work on both oversight and resource optimization.

## German Cyberspace Priorities and "Strategieunfähigkeit"

Germany has traditionally prioritized defense over offense in cyberspace. That's now beginning to change.

**There is a reoccurring debate in German** national security and foreign policy whether Germany suffers from "Strategieunfähigkeit"—an inability to develop and implement strategy. The historic trauma of two lost World Wars created a pacifist culture that always struggled with formulating national security interests and defining strategy. The so-called "culture of reluctance" regarding the use of hard power has bled into Berlin's thinking about cyber issues, especially as it rushes to develop capabilities without an overarching strategy on how to use them.

Until recently, Germany has prioritized defense over offense in cyberspace. The Federal Office for Information Security (BSI), Germany's cybersecurity agency, has a strictly non-military defensive mandate and is a vigilant advocate of strong encryption and full disclosure of zero-day vulnerabilities to vendors. Germany's foreign intelligence agency (BND) has historically had a relatively small cyber espionage budget.

Germany's defensive posture began to shift in 2015, after the internal network of the German Bundestag was successfully compromised by Russian state-backed operators. That led the country to revise its cybersecurity strategy, issuing a more offensive-minded document in 2016. It called for the development of cyber teams in the intelligence agencies. It also might have been a contributing factor to the creation of a specialized agency, called the Central Office for Information Technology in the Security Sphere (**ZITiS**), to develop innovative techniques to break into encrypted devices, develop exploits and malware for real time interception and accessing data at rest, as well as identify or purchase zero-days to support offensive capabilities.

As Germany rolled out its 2016 strategy, the German military (Bundeswehr) centralized its cyber capacity by consolidating around 14,000 soldiers and IT personnel into a unified cyber command (CIR), loosely modelled on U.S. Cyber Command. CIRwants to achieve full operational capacity by the early 2020s and plans to perform strategic and tactical cyber operations against enemy assets. Usage scenarios include disrupting enemy military assets, battlefield support and reconnaissance on adversary IT assets.

Through the new strategy, the meaning of cybersecurity in Germany shifted from strengthening IT-security to improving public safety through the use of offensive cyber operations.

Berlin's latest move favoring offensive cyber activity is the creation of a cyber innovation agency, akin to the United States' DARPA, announced in August 2018. Its mandate is to conduct market research and sponsor promising projects with potential value for cyber offense and cybersecurity. Over the next five years, the agency is supposed to be equipped with a budget of €200 million (roughly $227 million), 80 percent of which will fund research projects—a substantial sum considering that the entire budget of the BSI is only €120 million per year.

These developments over the last three years point to a build-up of Germany's offensive cyber capability. Interestingly, these new capabilities have been created without having a clearly defined strategic purpose—a problem that has plagued German national security policy in the past. For example, during the 2001 NATOmission in Afghanistan, Bundeswehr capabilities—

designed for territorial defense from invasion—were not well adapted or flexible enough for an expeditionary mission.

This mismatch between strategy and capabilities plagues Berlin's approach to cyberspace. There is currently no strategic debate about what German policymakers want to achieve with its new offensive capabilities. Questions about attribution and appropriate responses have apparently not yet been discussed. It is further unclear whether the political will exists to use these offensive capabilities in a time of crisis. For example, if deterring cyberattacks by punishment is a goal, strategy should make clear what means, including non-cyber options, would be most suitable. Is offensive cyber activity more useful in deterring adversarial cyber operations as say indictments or economic sanctions? Currently government officials seem to simply assume that cyber capabilities alone have a deterrent effect without taking into consideration the strategic requirements that come with deterrence by punishment, namely credibly holding assets at risk and signaling desired behavior while being willing to face consequences in case of an escalation. Will Germany indeed launch a retaliatory cyberattack against adversaries that provoke it and in turn face the potential consequences of entering an escalation cycle with, say, Russia or China?

As Germany tries to flex its muscles in cyberspace, allies and adversaries alike will be left to wonder what to expect absent an overall strategy. German policymakers should start a strategic discussion about the country's role in a contested cyberspace. It needs to explain to its allies how its new offensive tools will work to support multilateral frameworks like NATO, the EU and the UN. Germany also needs to signal to hostile cyber actors what behavior it deems inappropriate, and how it will likely respond if certain red-lines are crossed.

**Source**: Defense One

**Source**: Homeland Preparedness News

## Using Social Media to Weaken Impact of Terrorist attacks

A new report, Minutes to Months (M2M), assessed terror attacks in the United Kingdom, United States, Canada, New Zealand, and Australia. M2M reveals insights on how media and social media coverage can increase the public harms of terrorism, and what works to mitigate such effects. The research team found that terrorist attacks create shockwaves after the initial incident, as a wide range of voices compete through mainstream and social media. In fact, M2M found that communications after a terrorist incident often lead to a spike in hate crimes, extremism, and prompt damaging disinformation and rumors. Governments, police, and others involved in public safety need to be ready to offer accurate, regular information to minimize negative fallout, the researchers said. Terrorist violence, as the report explained, is intended to elicit intense and vivid reactions. Thus, by neglecting how to manage post-event situations is a current weak point in many governmental counter-terrorism frameworks. The increasing volume of communication channels allows different groups to voice alternative interpretations of the same event, causing multiple narratives and accounts circulating in the post-event environment.

Source: Homeland Security Newswire

## Google Maps Scammers Put their Own Phone Numbers onto Bank Listings

Google Maps lets users edit and update listings; crowd-sourcing has helped Google to fill in the details of its maps, such as adding new roads or parks: a helpful feature, particularly in areas where governments restrict distribution of such data or in what are often less-developed regions. However, it has also resulted in pranksters creating fake accounts that they then use to approve their own pranks. Previously, Google allowed people to submit changes to Google Maps via Map Maker: a service the company introduced in 2008 that let users worldwide upload new data to the company's online mapping service. The company closed Map Maker as of 31 March 2017 and absorbed many of its features into Google Maps. However, while Map Maker went away, the ability to edit maps did not. Using Local Guides, users can still add and edit places, share additional details about a place, moderate edits, view the status of their edits, and edit road segments. There have been multiple cases of Google Maps vandalism targeting bank details in the past month. A group of con artists based in Thane, a city just outside of Mumbai, has edited Maps listings to show their own contact numbers, then swindled sensitive account details out of the marks who called.

**Source**: Naked Security

## Combating Car Hacking with Cyber Security

Security gaps in modern vehicles could allow a remote hacker to take control of vehicles' computer systems and cause crashes. According to the British online newspaper the Independent, the makers of the Jeep Cherokee were forced to recall 1.4 million vehicles in 2015, after US researchers demonstrated they could remotely hijack a test car's computer system over the Internet during an experiment. According to Wired magazine, the test car was traveling 70 mph through a suburb of St. Louis, Missouri, when the researchers interfered with its air conditioning, radio and windshield wipers. The researchers then cut the transmission, so the car slowed to a stop after going 64 mph on a highway. Cars built after 2005 have between 50 and 100 electronic control units. They are essentially small computers that control many of the car's automated systems — everything from the locking system to the power steering and even the brakes.

It seems the nation is hurtling toward a future of driverless vehicles with huge strides made by Tesla, Waymo, Audi and eight other major automotive manufacturers. Even the US Army, through its Tank Automotive Research, Development and Engineering Center (TARDEC), is deep in the development of autonomous tanks. As a result, autonomous vehicles will add another layer of vulnerability on top of an already complicated system. From a national security perspective, the stakes have never been higher. According to Justin Cappos, a professor in the Computer Science and Engineering Department at New York University, an adversary with a mature cyberattack capability like Russia or China could kill millions of drivers and passengers in a coordinated cyber strike.

Grimm, a cybersecurity engineering and consulting firm in Michigan, designs security systems by asking: how do you know if your systems are vulnerable to cyberattacks; do other systems in a vehicle make you vulnerable to cyber attacks; is ransomware a concern for automotive security; what sort of communications go to and from your vehicle; and what are the threats to your system?

**Source**: In Homeland Security

## New Vehicle Hack Exposes Users' Private Data via Bluetooth

People who have synced their mobile phones with a wide variety of vehicle infotainment systems may have their personal information exposed to a new type of vehicle hack, security researchers say.

A researcher from Privacy4Cars, which offers a mobile app that can erase Personally Identifiable Information (PII) from modern vehicles, recently discovered that vehicles from several car makers can expose user data via the Bluetooth protocol.

Dubbed CarsBlues, the new vehicle hack, targets the infotainment systems in modern vehicles and allows an attacker to access user information within minutes, using only inexpensive and readily available hardware and software. No significant technical knowledge is required either, the company claims. Tens of millions of vehicles already in circulation worldwide are believed to be impacted, and the number continues to rise into the millions as more vehicles are evaluated. Exposed information includes contacts, call logs, text logs, and even full text messages in some cases.

Discovered by Privacy4Cars founder Andrea Amico, the hack mainly impacts users who synced their phones to vehicles that are no longer under their direct oversight. These include rented vehicles, as well as cars "shared through a fleet or subscription service, loaned, sold, returned at the end of a lease, repossessed, or deemed a total loss." "

Additionally, people who have synced their phones and given others temporary access to their personal vehicle, such as at dealerships' service centers, repair shops, peer-to-peer exchanges, and valets may also be at risk for CarsBlues," Privacy4Cars says.

**Source**: Security Week

## Bill that could Jail Executives who Mishandle Consumer Data

Senator Ron Wyden's draft proposal, called the Consumer Data Protection Act, would give the FTC more authority and resources to police the use of data by adding a total of 175 new staff. Under the proposal, the FTC would also be allowed to fine companies up to four percent of revenue for a first offense. The legislation would also create a centralized Do Not Track list meant to let consumers stop companies from sharing their data with third parties, or from using it for targeted advertising. The legislation would instead allow companies to block users who opt out and offer a paid version of the service in place of the tracking. Consumers could also ask to review and challenge the information collected on them. Companies that make more than $1 billion in revenue and that handle information on more than 1 million people, or smaller companies that handle information on more than 50 million people, would also be required to submit regular reports to the FTC that describe any privacy lapses. Failure to comply with the measure could lead to jail time.

**Source**: The Verge

# The US Military Just Publicly Dumped Russian Government Malware Online

Usually it's the Russians that dump its enemies' files. This week, US Cyber Command (CYBERCOM), a part of the military tasked with hacking and cybersecurity focused missions, started publicly releasing unclassified samples of adversaries' malware it has discovered.

CYBERCOM says the move is to improve information sharing among the cybersecurity community, but in some ways it could be seen as a signal to those who hack US systems: we may release your tools to the wider world.


"This is intended to be an enduring and ongoing information sharing effort, and it is not focused on any particular adversary," Joseph R. Holstead, acting director of public affairs at CYBERCOM told Motherboard in an email.

On Friday, CYBERCOM uploaded multiple files to VirusTotal, a Chronicle-owned search engine and repository for malware. Once uploaded, VirusTotal users can download the malware, see which anti-virus or cybersecurity products likely detect it, and see links to other pieces of malicious code.

One of the two samples CYBERCOM distributed on Friday is marked as coming from APT28, a Russian government-linked hacking group, by several different cybersecurity firms, according to VirusTotal. Those include Kaspersky Lab, Symantec, and Crowdstrike, among others. APT28 is also known as Sofacy and Fancy Bear.

Adam Meyers, vice president of intelligence at CrowdStrike said that the sample did appear new, but the company's tools detected it as malicious upon first contact. Kurt Baumgartner, principal security researcher at Kaspersky Lab, told Motherboard in an email that the sample "was known to Kaspersky Lab in late 2017," and was used in attacks in Central Asia and Southeastern Europe at the time.

"When reporting on it, Kaspersky Lab researchers noted it seemed interesting that these organizations shared overlap as previous Turla [another Russian hacking group] targets. Overall, it is not 'new' but rather newly available to the VirusTotal public."

The malware itself does not appear to still be active. A spokesperson for Symantec told Motherboard in an email that the command and control servers—the computers that tell the malware what commands to run or store stolen data—are no longer operational. The spokesperson added that Symantec detected the sample when the company updated its detection tools a couple of months ago.

CYBERCOM announced its new initiative on Monday, and uploaded its first two samples on the same day.

Source: Motherboard

## DHS to ID Critical Functions to Protect from Cyberattacks by Year's End

The Homeland Security Department hopes to complete a list of the nation's most vital functions that must be protected against cyberattacks before the end of this year. Once those "critical functions" are identified, Homeland Security will work with federal research facilities and other organizations to map out which of those functions are most vital and how they rely on each other. The broad goal for that mapping process is to identify which sectors rely most heavily on a critical function and what the chain reaction would be if a function was compromised by a cyberattack. Some sectors could continue functioning if GPS was compromised for a short period of time or had limited accuracy. Other sectors, such as the financial sector, which relies on GPS to pinpoint when securities trades happen, need 100 percent accuracy. The mapping process will likely begin with the telecommunications, energy, and finance sectors and other critical infrastructure sectors that are at greatest risks of enemy cyberattacks. The identification and mapping of critical functions is a project of Homeland Security's National Risk Management Center, which the department previously launched. The goal is for the center to tackle longer-range cyber problems that are out of scope for Homeland Security's cyber operations division.

**Source**: Nextgov

## FERC Approves 3 New Supply Chain Cybersecurity Standards

The Federal Energy Regulatory Commission (FERC) released a final rule last week approving three new Critical Infrastructure Protection (CIP) standards addressing supply chain risk management for bulk electric systems.

The new standards require responsible entities (distribution providers, generator owners and operators, transmission owners and operators) to develop and implement security controls for industrial control system hardware, software and services. These new standards respond to supply chain risks, including the insertion of counterfeit or malicious software, unauthorized production, tampering and theft.

According to the *National Law Review*, the new CIP standards will impose the following high-level requirements:

- **Cyber Security – Supply Chain Risk Management:** According to FERC, this standard "does not require any specific controls or mandate 'one-size-fits-all' requirements." Instead, this standard requires the development of a documented supply chain cyber security risk management plan for higher-risk covered systems that addresses, as applicable, six "baseline" security concepts:

  - Vendor security event notification;
  - Coordinated incident response;
  - Vendor personnel termination notification;
  - Product/services vulnerability disclosures;
  - Verification of software integrity and authenticity; and
  - Coordination of vendor remote access controls.

- **Cyber Security – Electronic Security Perimeter(s):** This standard will include two new requirements for identifying active vendor remote access sessions and having method(s) for disabling active vendor remote access sessions.

- **Cyber Security – Configuration Change Management and Vulnerability Assessments:** Finally, this standard requires responsible entities to verify the "identity of the software source and the integrity of the software obtained from the software source" prior to any installing software that changes established baseline configurations, "when methods are available to do so." According to NERC, these requirements could help reduce the risk that an attacker could "exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a [covered system]."

The final rule will take effect 60 days after it is published in the Federal Register, and the new standards must be implemented within 18 months.

**Source**: Security Magazine

## Apple Reportedly Blocked Police iPhone Hacking Tool

Apple's latest iteration of iOS has reportedly turned the GrayKey hacking device into an expensive doorstop. Law enforcement around the world has taken to using GrayKey to break into locked iPhones but it appears Apple has finally gotten ahead of the device's crafty manufacturers. For now.

Forbes' Thomas Brewster has been on top of the GrayKey saga from the beginning. On Wednesday, he cited sources from the forensic community who've told him that Apple's efforts to keep bad actors and law enforcement from cracking into its users' phones have paid off. According to the report, the $15,000 tool made by a shadowy company called Grayshift is now only capable of performing a "partial extraction" of data. It can pull a few unencrypted files and some metadata that's virtually worthless.

One source that went on the record for Forbes, Captain John Sherwin of the Rochester Police Department in Minnesota, confirmed that the release of iOS 12 has hobbled GrayKey's ability to unlock a phone. "That's a fairly accurate assessment as to what we have experienced," he told Forbes.

It's still unclear what exact change could have been made to shut GrayKey out. Previous reporting has told us that the tool uses a workaround to brute force its way in by guessing a users' password until it gets it right. Apple has protections in place to stop that kind of tactic and GrayShift's methods are a closely held secret. Not much is known about the company. In March, Forbes reported that GrayShift counts at least one ex-Apple security engineer as part of its team. You can't even view its website without a login given to members of law enforcement, though there have been indications that it works with private entities in some capacity as well.

With iOS 12, Apple implemented a highly-anticipated change called "USB Restricted Mode." This shuts off lightning port access on the iPhone if it hasn't been unlocked by a user in the last hour. This was widely believed to be Apple's solution to foil companies like GrayShift

and Cellebrite but we don't know for certain if that did the trick. Apple did not return our request for comment.

Whether it's the solution or not, you might want to double-check that your phone is set up for USB Restricted Mode. You'll need to be updated to iOS 12 and go to Settings > FaceID and


Passcode. Scroll down to the bottom of the page and you want your settings to look like this: There's no word on whether GrayShift's competitors have hit a wall in their efforts to subvert Apple's security. This is a big money business and we can expect that whoever loses their cash cow will be working overtime to figure out another workaround.

**Source**: Gizmodo

## 83% Avoid a Business Following Breach and 21% Never Return

Almost half (44%) of US consumers have suffered the negative consequences of a security breach or hack, according to new research conducted on behalf of secure payments provider to contact centers, PCI Pal. The findings suggest that the combination of high-profile recent breaches, headlines devoted to new data privacy regulations such as the GDPR and California Privacy Law, and personal experience have put security concerns front and center for American shoppers.

"While security breaches are not new, US consumers' attitudes towards them seem to be changing significantly - with the vast majority of Americans now reporting that trust in security practices (or lack thereof) influences not just where but also how, and how much they spend," explained James Barham, COO at PCI Pal.

The research found that 83% of consumers will stop spending with a business for several months in the immediate aftermath of a security breach or a hack. Even more significantly, over a fifth (21%) of consumers will never return to a brand or a business post-breach, representing a significant loss of revenue. For any consumer facing business, this figure offers a stark warning.

Consumers reported that even being perceived as having lax security practices can be enough to incur spending penalties - almost half (45%) reported that they spend less with brands they perceive to have insecure data practices, while over a quarter (26%) say they stop spending completely if they don't trust a company with their data.

The findings suggest that it's not just online threats that worry consumers - 28% question how their data is being recorded when on the phone and almost half (42%) are uncomfortable sharing sensitive data such as credit card details over the phone. Given that 66% of all call centers are based in The Americas, the burden of security provisions to mitigate these concerns, must be a focus for organizations and brands that rely on telephone customer service practices.

Barham continues: "What's really interesting is how consumers are increasingly questioning data security practices. 61% know they should check a company's security process and 28% say they question businesses directly or research how they safeguard consumer data. This suggests a real change in how consumers prioritize privacy and security. Consumer-facing brands should pay attention - not just adopting stronger security practices but incorporating them into their marketing and communications strategies if they want to keep customers loyal and spending with them."

**Source**: Security Magazine

## NIST to use IBM's Watson AI system to score vulnerabilities

The U.S. National Institute of Standards and Technology (NIST) reportedly plans to replace its method of scoring publicly disclosed vulnerabilities with a new automated process leveraging IBM's Watson artificial intelligence system.

The agency expects Watson to supplant its current Common Vulnerability Scoring System (CVSS) process for most bugs by October 2019, according to a report from Nextgov, citing Matthew Scholl, chief of NIST's computer security division. IBM has confirmed this account to SC Media, which has also reached out to Scholl for additional comment.

A key advantage of using AI is that it should ease the burden of NIST analysts who are currently tasked with reviewing thousands of vulnerabilities every week.

"Artificial Intelligence is solving the manual effort problem that many organizations face. For security leaders, it's important to know that not all AI is equal, but when the right choice is made, the benefits from a time, cost, and resource perspective can be immense," said George Wrenn, CEO at CyberSaint Security, a company specializing in automated intelligent cybersecurity compliance. "It is no surprise NIST is delving into this area," he added in emailed comments.

Reportedly, Watson participated in a pilot program earlier this year in which it processed hundreds of thousands of older vulnerabilities and corresponding CVSS scores, and then asked to score new vulnerabilities based on that precedent. Whenever the new bug was similar to a previously studied vulnerability, Watson fared very well, scoring the flaw similar to how a person would.

But if the bug was something unique or highly complex, like the Spectre vulnerability that was discovered earlier this year, Watson reportedly struggled. As a fail-safe for this issue, Watson will produce a confidence percentage for each score. If the AI engine's confidence percentage falls under the high 90s, the human analyst will take over the review, and edit the risk score accordingly.

Gabriel Gumbs, VP of product strategy at STEALTHbits Technologies, said in emailed comments that NIST's use of Watson holds even more potential.

"Applying AI, and in particular Watson to the scoring of vulnerabilities will be useful for keeping up with the increased NIST workload; however, I don't foresee this addressing the issue of organizations still not patching their systems in time," said Gumbs. "In theory, the ranking of vulnerabilities helps prioritize which systems in first and how soon those patches are applied. I believe this program could go a step further and score both the inherit risk, and the residual risk of vulnerabilities when other controls are in place. This would allow for real-world patch prioritization scenarios where organizations can apply controls that can be rolled out faster than a patch, and in cases where patches do not [yet] exist still reduce their exposure."

**Source**: SC Magazine

## Hackers Erase 6,500 Sites From the Dark Web in One Attack

One of the most popular Dark Web hosting services – Daniel's Hosting – was slaughtered last week when attackers hosed it clean of about 6,500 hidden services. The admin says they're gone for good: he hasn't even figured out where the vulnerability is yet.

The administrator at Daniel's Hosting is a German software developer named Daniel Winzen, who acknowledged the attack on the hosting provider's portal. Winzen said that it happened on Thursday night, a day after a PHP zero-day exploit was leaked.

The service will likely be back in December, he said, but even the "root" account has been deleted, and all the data on those 6,500 sites are toast:

> There is no way to recover from this breach, all data is gone. I will re-enable the service once the vulnerability has been found, but right now I first need to find it.

Backups? Forget it. This is the Dark Web. Winzen told ZDNet that there ain't no such thing as backups on Daniel's Hosting, by design:

> Unfortunately, all data is lost and per design, there are no backups.

As of last week, Winzen said his priority was to do a full analysis of the log files. He had determined that the attacker(s) had gained administrative database rights, but it's looking like they didn't get full system access. Some accounts and files that weren't part of the hosting setup were left "untouched," he said.

Other than the root account, no accounts unrelated to the hosting were touched and unrelated files in `/home/` weren't touched either. As of now there is no indication of further system access and I would classify this as a "database only" breach, with no direct access to the system. From the logs it is evident that both, adminer and phpmyadmin have been used to run queries on the database.

**Who cares?**

According to Dark Owl, when the attacker(s) took out Daniel's Hosting, they erased over 30% of the operational and active hidden services across Tor and the Invisible Internet Project (I2P) – an anonymous network layer that allows for censorship-resistant, peer-to-peer communication. ZDNet's Catalin Cimpanu tweeted on Monday night that this pretty much matched his own calculations.

The attacker(s) also deleted over six million documents that DarkOwl – a provider of darknet content and tools, as well as cybersecurity defenses – had archived on the Dark Net.
This is what the world lost when Daniel's Hosting went belly-up, Dark Owl says:

- 657 of the hidden services had the title *"Site Hosted by Daniel's Hosting Service"* and little else (but may have been used for something other than serving web content).
- Most (over 4900) were in English, 54 were in Russian and two of the oldest were in Portuguese.
- 457 of the hidden services contain content related to hacking and/or malware development.
- 304 have been classified as forums.
- 148 of them are chatrooms.
- 136 include drug-specific keywords.
- 109 contain counterfeit-related content.
- 54 specifically mention carding-specific information.
- Over 20 contain content including weapons and explosive-related keywords.

For better or worse, the takedown of Daniel's Hosting means that a "pillar of the darknet community" that's served up a chatroom and online-link list for years, free of charge, has been demolished, Dark Owl says.

For example, his online-link list is referenced by nearly 500 other hidden services, making it the second most commonly referred to directory listing (behind Fresh Onions) and providing a foundational starting point for new users navigating Tor.

Dark Owl has some theories about who could have been behind the attack. It could have been Russian hackers, who've recently outlined the technical details of exploiting PHP's `imap_open()` function to extract password hashes for privileged accounts, as an alternative to brute-force mining.

Then again, it could have been anybody who's against easy posting and sharing of child abuse images. Dark Owl reports that Winzen, back in 2016, made life easier for people to share such images on Tor without potentially exposing their identities:

As a result, Daniel's LE-Chat code became a popular platform for the darknet pedophilia community, and the home for many well-known Child Pornography sharing chatrooms such as Tabooless, Camp Fire, and Child Priori.

There are also theories about the portal being taken down by law enforcement. For one thing, a chatroom, Daniel's Chat, quietly resurfaced on Saturday, but it lacked the member database and credentials that had enabled users to verify chat participants' identities.

Or perhaps Daniel had been arrested, and it's not even really him who's posting on the site and sending email to news outlets? As it is, the providers' hidden services experienced what Dark Owl said was "extreme" distributed denial of service (DDoS) attacks leading up to the attack, "similar to other law enforcement-led darknet seizure operations."

Those are just some of the theories.

The attack shows how surprisingly centralised the Dark Web really is, and that there are no ironclad promises that its potent anonymity features will shield you.

Whether it's law enforcement catching drug dealers with a fake Bitcoin exchange or simple misconfigurations that expose server IP addresses, you have to take heed: just because you're using Tor doesn't necessarily mean you're safe, whether you're a criminal or somebody seeking anonymity for noncriminal reasons.

There are many ways to get busted on the dark web.

**Source**: Naked Security

## USPS Took a Year to Fix a Vulnerability That Exposed All Users' Data

The US Postal Service says it's fixed a security weakness on usps.com that let anyone see the personal account info of its users, including usernames and street addresses. The open vulnerability was reportedly identified over a year ago by an independent researcher but USPS never patched it until this week, when Krebs on Security flagged the issue.

The vulnerability included all 60 million user accounts on the website. It was caused by an authentication weakness in the site's application programming interface (API) that allowed anyone to access a USPS database offered to businesses and advertisers to track user data and packages. The API should have verified whether an account had permissions to read user data but USPS didn't have such controls in place.

Users' personal data including emails, phone numbers, mailing campaign data were all exposed to anyone who was logged into the site. Additionally, any user could request account changes for another user, so they could potentially change another account's email address and phone number, although USPS does at least send a confirmation email to confirm the changes.

""NO SPECIAL HACKING TOOLS WERE NEEDED TO PULL THIS DATA.""

Since street addresses are searchable through the database, any logged-in user could see who was living at each residence and even gain the data of multiple people in the same household. Krebs notes that because of the vulnerability, "no special hacking tools were needed to pull this data."

USPS said in a statement to Krebs: “Any information suggesting criminals have tried to exploit potential vulnerabilities in our network is taken very seriously. Out of an abundance of caution, the Postal Service is further investigating to ensure that anyone who may have sought to access our systems inappropriately is pursued to the fullest extent of the law.” A recent audit of its system in October did not turn up this vulnerability, although it did find numerous other weaknesses. We’ve reached out for comment on whether USPS was aware of the issue when it was initially noted over a year ago. So far, no known exploits were made through this vulnerability.

In USPS’ continued efforts to modernize and adapt to the digital age, it’s faced numerous cybersecurity challenges. In 2014, a hack affected 800,000 USPS employees and 2.9 million records of customer service inquiries.

**Source**: The Verge

## VirtualBox Zero-Day Vulnerability Details and Exploit Are Publicly Available

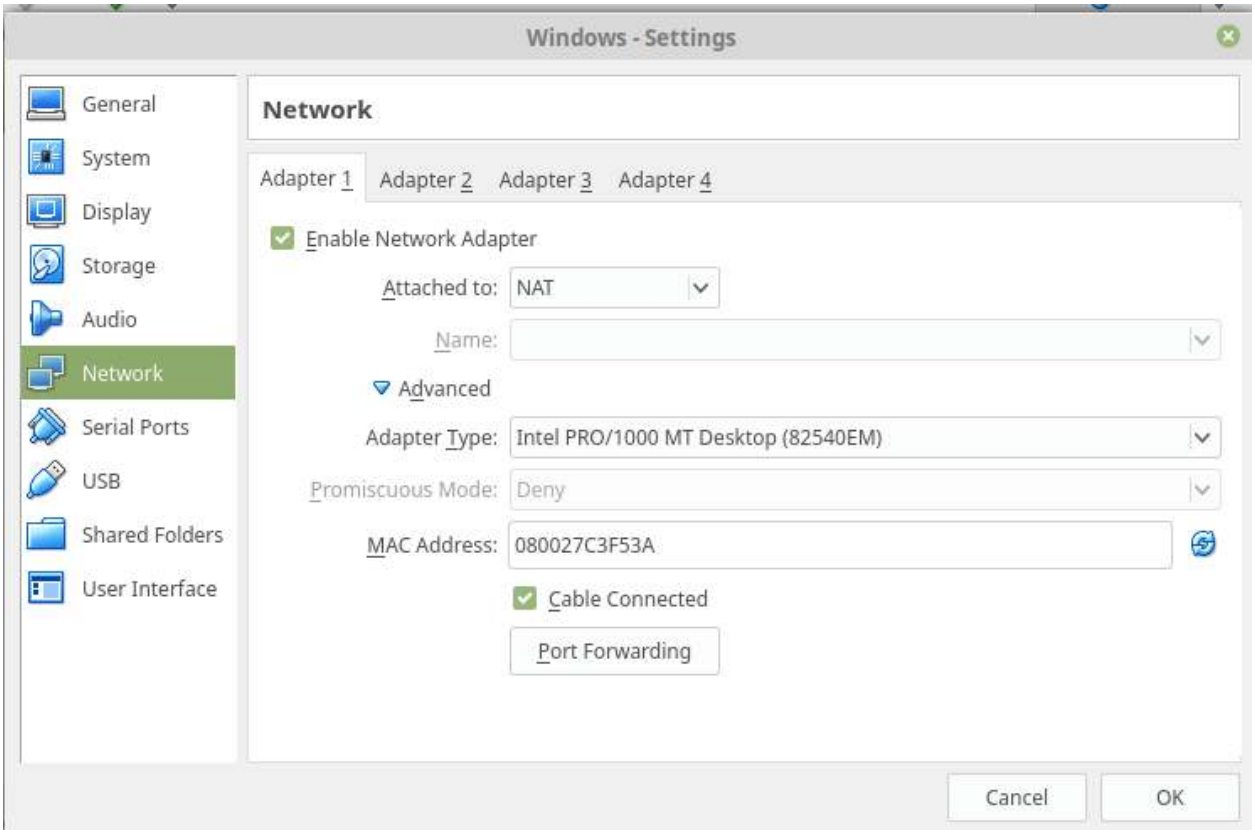
A Russian vulnerability researcher and exploit developer has published detailed information about a zero-day vulnerability in VirtualBox. His explanations include step-by-step instructions for exploiting the bug.

According to the initial details in the disclosure, the issue is present in a shared code base of the virtualization software, available on all supported operating systems.

Exploiting the vulnerability allows an attacker to escape the virtual environment of the guest machine and reach the Ring 3 privilege layer, used for running code from most user programs, with the least privileges.

**Turning one "overflow" into another**

Sergey Zelenyuk found that the security bug can be leveraged on virtual machines configured with the Intel PRO/1000 MT Desktop (82540EM) network adapter in Network Address Translation (NAT) mode, the default setup that allows the guest system to access external networks.




"The [Intel PRO/1000 MT Desktop (82540EM)] has a vulnerability allowing an attacker with root/administrator privileges in a guest to escape to a host ring3. Then the attacker can use existing techniques to escalate privileges to ring 0 via /dev/vboxdrv," Zelenyuk writes in a technical write-up on Tuesday.

Zelenyuk says that an important aspect in getting how the vulnerability works is to understand that context descriptors are processed before data descriptors.

The researcher describes the mechanics behind the security flaw in detail, showing how to trigger the necessary conditions to obtain a buffer overflow that could be abused to escape the confinements of the virtual operating system.

First, he caused an integer underflow condition using packet descriptors - data segments that allow the network adapter to track network packet data in the system memory.

This state was then leveraged to read data from the guest OS to into a heap buffer and cause an overflow condition that could lead to overwriting function pointers; or to cause a stack overflow condition.

**100% reliable exploit**

The exploit Zelenyuk wrote relies on the two overflow conditions. Since it provides access to Ring 3 level of permissions, privilege escalation is needed to take control over the host operating system.

Although this is not impossible, an attacker has to chain another vulnerability that would grant them increased privileges on the system.

The steps described by the researcher for exploiting the zero-day he uncovered in VirtualBox are definitely not script-kiddie-friendly as they require more advanced technical knowledge.

Buffer overflows are not always stable and most of the times they result in crashing the target. However, Zelenyuk says that his exploit is "100% reliable," and it "it either works always or never because of mismatched binaries or other, more subtle reasons I didn't account."

He tested his work on Ubuntu 16.04 and 18.04, both 86- and 64-bit with the default configuration. Proof of the success is the following video that shows the exploit running in the guest OS and executing a shell on the host OS:

This is not the researcher's first vulnerability disclosure in VirtualBox. Earlier this year, he reported another security bug in VirtualBox. It was reported responsibly for version 5.2.10 of the software. For some reason, though, Oracle fixed the problem silently in version 5.2.18 of its hardware virtualization software and did not give credit to the researcher for finding and reporting the vulnerability.

At the beginning of today's report, Zelnyuk clearly states the reasons that drove him to publicly announcing the full details for the current zero-day, before informing the developer of the issue. Oracle's past reaction to his reporting seems to have played a part in this.

1. Wait half a year until a vulnerability is patched is considered fine.
2. In the bug bounty field these are considered fine:
    1. Wait more than month until a submitted vulnerability is verified and a decision to buy or not to buy is made.
    2. Change the decision on the fly. Today you figured out the bug bounty program will buy bugs in a software, week later you come with bugs and exploits and receive "not interested".
    3. Have not a precise list of software a bug bounty is interested to buy bugs in. Handy for bug bounties, awkward for researchers.
    4. Have not precise lower and upper bounds of vulnerability prices. There are many things influencing a price but researchers need to know what is worth to work on and what is not.
3. Delusion of grandeur and marketing bullshit: naming vulnerabilities and creating websites for them; making a thousand conferences in a year; exaggerating importance of own job as a security researcher; considering yourself "a world saviour". Come down, Your Highness.

I'm exhausted of the first two, therefore my move is full disclosure. Infosec, please move forward.

**Source**: Bleeping Computer