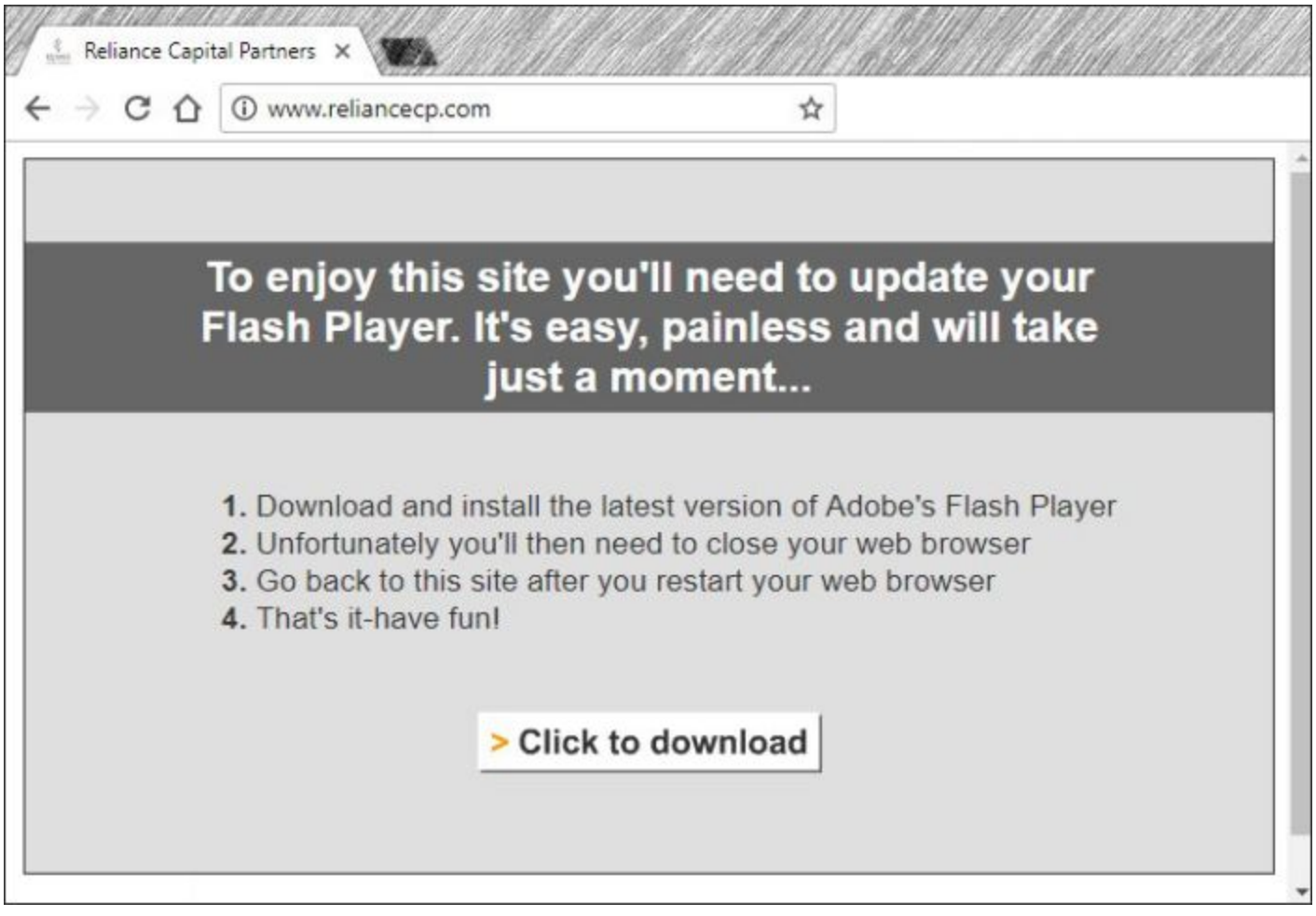
Security Now! #697 - 01-15-19

Zerodium

This week on Security Now!

This week we examine the intended and unintended consequences of last week's Windows Patch Tuesday, and speaking of unintended consequences, the US Government shutdown has had some, too! We also examine a significant privacy failure in WhatsApp, another Ransomware decryptor (with a twist), movement on the DNS-over-TLS front, an expectation of the cyberthreat landscape for 2019, a cloudy forecast for The Weather Channel App, a successful 51% attack against the Ethereum Classic cryptocurrency, another court reversing compelled biometric authentication, and an update on the lingering death of Flash... now in hospice care. We then look at a bit of miscellany and Errata and finish by examining the implications of the recent increase in bounty for the purchase of 0-day vulnerabilities.



Security News

Microsoft Patch Tuesday Redux

Last week's Patch Tuesday fixed 51 vulnerabilities, seven of them rated Critical.
It also broke Windows file sharing for Windows 7 and Server 2008 R2... but we'll get to that in a second. First, the good news:

There was a surprising DHCP vulnerability discovered internally by Microsoft's own enterprise security group that could allow an attacker to send a specially crafted DHCP response to a client in order to perform arbitrary code execution on the client. They wrote: "A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client. An attacker who successfully exploited the vulnerability could run arbitrary code on the client machine. To exploit the vulnerability, an attacker could send a specially crafted DHCP responses to a client." Whoops. DHCP is promiscuous enough that this could have been a big problem.

Last week's updates also closed a pair of Hyper-V vulnerabilities that could have allowed powerful escapes from virtualization. Microsoft wrote: "To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code."

Three of the other critical flaws patched were in the ChakraCore scripting engine that fails to properly handle objects in memory in Edge, and the last glitch was a publicly disclosed but not observed in wild vulnerability in the Jet database engine that could have allowed by remote code execution.

However, as has become all too commonplace lately, included in last Tuesday's release were two updates that caused problems connecting to network shares on Windows 7 and its server version, Windows Server 2008 R2. Three days later, last Friday the 11th, Microsoft released a a stand-alone update to resolve the problem introduced by Tuesday's patches:

The two updates that caused this problem are KB4480960 and KB4480970. After they were applied, local users who were part of the local "Administrators" group were unable to connect to remote shares on Windows Server 2008 R2 or Windows 7 Machines.

The subsequent release of stand-alone update KB4487345 reverses this problem. So... anyone who has been unable to connect to remote shares since January's patch Tuesday updates were installed should download and install KB4487345:

https://www.catalog.update.microsoft.com/Search.aspx?q=KB4487345

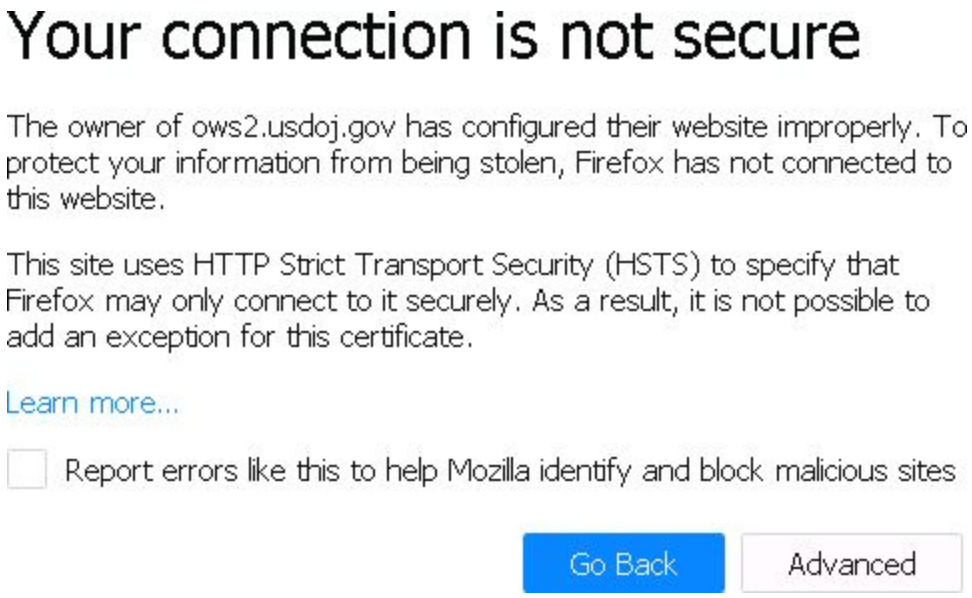
It's a small ~20 megabyte update that'll fix you right up!

(There was an interim workaround registry tweak that some users applied to fix the problem. If that was done be sure to remove the registry "LocalAccountTokenFilterPolicy" REG_DWORD that was created after the proper fix has been applied.)

Also last week, Windows 7 machines being activated through Microsoft's Key Management Service (KMS) began receiving "Windows is not genuine" notifications indicating that the Windows license was not valid. Due to its coincidence with patch Tuesday, the initial suspicion was that in addition to file sharing, KMS activation had also been broken by Tuesday's updates. But it later turned out that this this problem resulted from a mistaken change to Microsoft's activation servers. Microsoft explained THAT one by writing:

"A recent update to the Microsoft Activation and Validation unintentionally caused a "not genuine" error on volume-licensed Windows 7 clients that had KB 971033 installed. The change was introduced at 10:00:00 UTC on January 8, 2019, and was reverted at 4:30:00 UTC on January 9, 2019."

Government shutdown: TLS certificates not renewed, many websites are down
As our US listeners know, at the time of this podcast the U.S. government is partially shutdown due to a political funding dispute over the proper nature of the enforcement of security at the Southern US border. In a classic example of unintended consequences, a growing number -- somewhere around 80 and counting -- government websites are no longer accessible, or have been marked as using insecure connections, because, during this government outage, their server's TLS certificates have expired and cannot be renewed until the government reopens.



And, to further confuse matters, .gov websites with expired certificates which are also on the HSTS preload list (see example above), including all of the usdoj.gov subdomains, are completely inaccessible by Chrome and Mozilla because they remove any option to "run a bypass" for any site that has asked to only ever be accessed securely.

Whoopsie.

While the shutdown draws on, additional sites are expected to join the ranks of those which are inaccessible. Since these US Government shutdowns are becoming more commonplace than

rare, but since we can also always see them approaching, the takeaway here for the future is for any admins of such sites to check their certs BEFORE things get politically locked up and get near-expiring certificates reissued before rather than after.

Other sites, for example https://rockettest.nasa.gov/ and https://d2l.lbl.gov (Lawrence Berkeley National Laboratory) also have unexpired certs but no HSTS protection. After the sites lost their certs (the NASA site on January 5th and LBL on the 8th) they were initially accessible by forcing past browser warnings. But in the case of logins, this exposed the users' login credentials. When I checked this morning, DNS had been pulled from the rockettest.nasa.gov domain and traffic was being blocked to ows2.usdoj.gov. So someone was still around to at leave prevent HTTPS bypass abuse of the site, if not to get certs reissued.

Does WhatsApp Has A Privacy Bug That Could Expose Your Messages?
https://thehackernews.com/2019/01/whatsapp-privacy-chats.html

Last Friday an Amazon employee tweeted about an incident that many have suggested could be an indication of a significant privacy bug in the most popular end-to-end encrypted, Signal-based, Whatsapp messaging app. The apparent leakage of someone else's Whatsapp messaging stream into Addy Fuller's certainly should raise privacy concerns.

According to Abby Fuller, she found some mysterious messages on WhatsApp, which were not associated with her contacts, immediately after she created a new account on her new phone using a new number for the first time.

Abby believed that the mysteriously appeared content on her new account was the message history associated with the WhatsApp account of the previous owner of the same SIM/mobile number, which WhatsApp pushed to her phone... and, unfortunately, she was almost certainly correct.

As we know, WhatsApp uses our phone number as our authentication in lieu of any username and password, and the argument has been that since Whatsapp only sends to that number, it's not a vulnerability. But what exactly happens when phone numbers change hands?

It's clear from an online FAQ that Whatsapp is aware of this issue. The problem is that its users aren't aware and they've made everything so simple and automatic that it's difficult to then ask users to pay attention to something that's far from obvious:

https://faq.whatsapp.com/en/s40/28030001/

> *Changing phone numbers and/or phones / Changing your WhatsApp phone number*
>
> *Before you stop using a particular phone number, you should migrate your WhatsApp account to the new number. For a simple way to do this, use our Change Number feature. By using this feature, you'll be able to migrate your account information (including your profile information) as well as your groups.*
>
> *Make sure your contacts delete your old phone number from their phone's address book and input your new number. As it is a common practice for mobile providers to recycle numbers, you should expect that your former number will be reassigned.*

Abby's tweets indicated that the chat history she received on her new phone was "not FULL, but definitely actual threads/DM conversations." We know that Whatsapp doesn't archive messaging on their servers, but we do know that undelivered messages will persist in encrypted form for up to 45 days.

The other problem is that once a device's SIM and phone number have been used to establish the local device's encryption keys, the SIM can be removed and returned, yet that device, now absent cellular telephony, can continue to use the encryption keys it still has until such time as the phone number associated with its absent SIM becomes assigned to some other Whatsapp user.

And THAT rather glaring loophole, combined with storage and catch-up delivery of pending messages creates an opportunity for significant user privacy leakage.

The way Whatsapp operates, the system trusts new encryption keys broadcasted by a contact and uses it to automatically re-encrypt undelivered messages and send them to the recipient without informing or leaving an opportunity for the sender to verify the recipient.

And this, of course, brings us back to my #1 complaint about the ease-of-use / security / privacy tradeoff we inevitably encounter anytime someone else manages our keys for us. I like Threema because they keep this in the hands of their users. All of these systems's have keys, that's the way today's crypto works. There's no getting around it. So if I were to coin a phrase to be a perfect corollary to our TNO (Trust No One) it would be:

If you're not managing your own keys... someone else is.

The moral of this incident is: If you, or those you are responsible for, are using Whatsapp, be sure to proactively transfer your own account to a new device BEFORE releasing the phone number of the device you are using. If you don't, whomever obtains your number and uses it to create a Whatsapp account may obtain access to your previous private messages.

PyLocky Ransomware Decryption Tool Released — Unlock Files For Free
https://thehackernews.com/2019/01/pylocky-free-ransomware-decryption.html
... or probably not!

I got a huge kick out of this story. "Unlock Files For Free!" I figured this would be another of those recent reports of file encryption being done wrong where it's possible to create a file decrypter to perform after-the-fact decryption of previously encrypted files.

If your computer has been infected with PyLocky Ransomware and you are searching for a free ransomware decryption tool to unlock or decrypt your files—your search might end here.

Security researcher Mike Bautista at Cisco's Talos cyber intelligence unit have released a free decryption tool that makes it possible for victims infected with the PyLocky ransomware to unlock their encrypted files for free without paying any ransom.

((Possible... yes... probable? Uhhhhhhhhhh.....))

The decryption tool works for everyone, but it has a huge limitation—to successfully recover your files, you must have captured the initial network traffic (PCAP file) carried out between the PyLocky ransomware and its command-and-control (C2) server, which generally nobody purposely does.

((Yeah, no kidding.))

This is because the outbound connection—when the ransomware communicates with its C2 server and submit decryption key related information—contains a string that includes both Initialization Vector (IV) and a password, which the ransomware generates randomly to encrypt the files.

Cisco's researcher explains: "If the initial C2 traffic has not been captured, our decryption tool will not be able to recover files on an infected machine. This is because the initial callout is used by the malware to send the C2 servers information that it uses in the encryption process."

First spotted by researchers at Trend Micro in July last year, PyLocky ransomware found spreading through spam emails, like most malware campaigns, designed to trick victims into running the malicious PyLocky payload.

January 9, 2019: Google Public DNS now supports DNS-over-TLS
https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html

<quote> "We implemented the DNS-over-TLS specification along with the RFC 7766 recommendations to minimize the overhead of using TLS. These include support for TLS 1.3 (for faster connections and improved security), TCP fast open, and pipelining of multiple queries and out-of-order responses over a single connection. All of this is deployed with Google's serving infrastructure which provides reliable and scalable management for DNS-over-TLS connections."

They also note that: Android 9 (Pie) device users can use DNS-over-TLS today. For configuration instructions for Android and other systems, please see the documentation. Advanced Linux users can use the stubby resolver from dnsprivacy.org to talk to Google's DNS-over-TLS service.

https://developers.google.com/speed/public-dns/docs/using
https://developers.google.com/speed/public-dns/docs/dns-over-tls

When using a strict privacy profile, stub resolvers establish a DNS-over-TLS connection with the following steps.

1. The stub resolver is configured with the DNS-over-TLS resolver name dns.google.

2. The stub resolver obtains the IP address(es) for dns.google using the local DNS resolver.

3. The stub resolver makes a TCP connection to port 853 at the one those IP address.

4. The stub resolver initiates a TLS handshake with the Google Public DNS resolver.

5. The Google Public DNS server returns its TLS certificate along with a full chain of TLS certificates up to a trusted root certificate.

6. The stub resolver verifies the server's identity based on the certificates presented. If the identity cannot be validated, DNS name resolution fails and the stub resolver returns an error.

7. After the TLS connection is established, the stub resolver has a secure communication path between to a Google Public DNS server.

8. Now the stub resolver can send DNS queries and receive responses over the connection.

DoT vs DoH...

- We already have DoH Support (DNS over HTTPS)
- Browsers: Firefox, Chrome
- Tools: Curl
- Phones: Android P
- Services: Cloudflare, Google , PowerDNS ....

https://dnsprivacy.org/wiki/display/DP/Windows+installer+for+Stubby

Their paper is titled: A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth
https://arxiv.org/pdf/1901.00846.pdf

We're all familiar with the expression "crime doesn't pay." The point, I think, is that getting caught eventually makes any crime, which may have appeared to be going along nicely up until that point, suddenly a source of regret. That adage could certainly apply to those who are behind efforts to steal others' computing resources for the mining of cryptocurrency... because as this paper successfully demonstrates, until these miscreants are caught, their crimes appear to be paying off rather handsomely.

Abstract:
Illicit crypto-mining leverages resources stolen from victims to mine cryptocurrencies on behalf of criminals. While recent works have analyzed one side of this threat, i.e.: web-browser cryptojacking, only white papers and commercial reports have partially covered binary-based crypto-mining malware. In this paper, we conduct the largest measurement of crypto-mining malware to date, analyzing approximately 4.4 million malware samples (1 million malicious miners), over a period of twelve years from 2007 to 2018. Our analysis pipeline applies both static and dynamic analysis to extract information from the samples, such as wallet identifiers and mining pools. Together with [open source intelligence] data, this information is used to group samples into campaigns. We then analyze publicly-available payments sent to the wallets from mining-pools as a reward for mining, and estimate profits for the different campaigns.

Our profit analysis reveals campaigns with multi-million earnings, associating over 4.3% of Monero with illicit mining. We analyze the infrastructure related with the different campaigns, showing that a high proportion of this ecosystem is supported by underground economies such as Pay-Per-Install services. We also uncover novel techniques that allow criminals to run successful campaigns.

So... what's the cash out value of 4.3% of the moneros in circulation?

It's a tidy $56 million USD.

In their outlook for 2019, Check Point Security sees cryptocurrency stealing software continuing to be the most commonly distributed form of malware. All of the top slots in Check Point's top ten list of the most prominent malware were currency miners. Coinhive continues to be the most prominently distributed malware, followed by XMRig, both of which use the victim computer to mine Monero with the profits directed into the crypocurrency wallet of the attacker. They are

followed by Jsecoin, a JavaScript miner embedded into websites, then Cryptoloot -- a direct competitor to Coinhive. Cryptoloot was second only to Coinhive during November, but its distribution has since dropped a bit.

AVAST's Threat Landscape Report for 2019
https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf

26 pages. The Internet of Things section has a subsection with the headline: "Router-based Attacks - the worst is yet to come."

Anyone whose home is connected to the internet has a router to which they can connect their computers, phones, and IoT devices. Routers are ubiquitous devices - important but rarely maintained to the latest security standards. In fact, once an internet service provider has installed it, most people never give their router a second thought, unless they experience internet disruptions. Avast research shows that 60% of users around the world have never updated their router's firmware, leaving them potentially vulnerable to fairly simple attacks that exploit firmware vulnerabilities.

Infected routers don't necessarily show signs of weakness. When an attacker uses a known vulnerability or weak authentication credentials to access a router, they can gain access not just the router but to all the devices connected to the network. Many users, therefore, may not be aware that their home network has been infiltrated. Routers have proven to be a simple and fertile target for a growing wave of attacks. While many attacks against routers use variants based on the Mirai codebase (which was released by the creator shortly after the successful attacks of September 2016), many are far more complex and point to a murky future for home network security.

Not only have we seen an increase in router-based malware in 2018, but also changes in the characteristics of those attacks. Where router-based malware has traditionally taken over a device for the purposes of carrying out a DDoS attack, such as the Mirai attacks, today's attacks use malware that infects a device and then opens up a line of communication to a command and control server without taking any immediate action.

We saw this with VPNFilter and Torii; once the router is infected, these malware strains listen to the network traffic, fingerprint the network and the devices on it, and allow for the command and control server to send new payloads or instructions to the device. In this, the malware acts more like a platform and less like a virus. This 'platform-ification' of IoT malware opens up many possibilities for bad actors who can re-purpose it for a multitude of nefarious activities including pay per install, DDoS for hire, cryptomining, or even good old-fashioned spam. This evolution replicates how PC malware counterparts have evolved and indicates the sophistication of new strains of IoT targeted malware.

In 2019, we expect to see hijacked routers used to steal banking credentials, for example, where an infected router injects a malicious HTML frame to specific web pages when displayed on mobile. This new element could ask mobile users to install a new banking app, for instance, and the malicious app will then capture authentication messages. In 2018, we observed a content injection method with coinmining elements on Mikrotik routers, and in 2019, we expect to see

this both escalate in number and to diversify in how content injection capabilities are used.

The good news is, the now nearly universal use of HTTPS will almost completely thwart MITM injection. But there are still places where HTTPS hasn't gone, most notably, eMail. Where people use web-based they are protected inside the HTTPS wrapper. And the use of encrypted connections to old school POP3, IMAP and SMTP eMail servers is on the rise. All of GRC's eMail clients are connecting over TLS links.

NetGate's SG-1000 has been replaced by the SG-1100, for $159.00
https://store.netgate.com/pfSense/SG-1100.aspx

- 5x packet processing performance gain vs. the SG-1000
- First product equipped with Microchip® CryptoAuthentication Device which provides assurance your system is running authentic, unaltered pfSense software
- 3x GbE Ethernet (WAN/LAN/OPT)

A Cloudy forecast for The Weather Channel App
https://int.nyt.com/data/documenthelper/554-l-a-weather-app-location/8980fd9af72915412e31/optimized/full.pdf

Los Angeles has sued The Weather Channel (TWC), claiming that it's been posing as a "personalized local weather data, alerts and forecasts" app... but in truth makes profits by tracking users "throughout the day and night" so as to sell their private, personal location data.

The lawsuit calls The Weather Company's practices "fraudulent and deceptive" and says they violate California's Unfair Competition Law. TWC fails to disclose that it collects users' location data and sends it to third parties, the suit maintains.

LA says: "It isn't about analyzing the clouds above our heads for a personalized weather forecast. Rather, it's about collecting location data for "advertising and other commercial purposes unrelated to weather data, alerts and forecasts."

None of the marketing purposes of collecting geolocation data are disclosed on either Apple's App Store or Google's Android Play Store versions of the free app, which is also available in an ad-free version for $3.99, the lawsuit notes.

When users download the app, TWC prompts them to allow it to access their location data, but it doesn't say anything about sharing that data, the lawsuit says:

The permission prompt also fails to reference or link to any other source containing more detailed information about what users' geolocation information will be used for.

The app's privacy policy does note that data could be used for targeted advertising and might be shared with "partners," the lawsuit says. But why would users even think to look at the policy, given that the prompt doesn't mention that their data will be used in those ways?

The lawsuits alleges that: "Unbeknownst to users," TWC's core business is "amassing and profiting from user location data." The lawsuit refers to a 2016 article that describes TWC as a "location data company powered by weather."

The lawsuit asserts that TWC's failure to alert users that their personal information is being sold is "no mere oversight." It quoted Domenic Venuto, General Manager, Consumer Division at TWC, who admitted in an interview that…

[If] a consumer is using your product and says 'Hey, wait a minute, why do they want to know where I am?' because it isn't an organic fit with the app, you are going to have some problems.

(In other words, we all expect a Weather App to need to know where we are for obvious reasons, and NOT so that it can resell our every movement.)

Last month, a New York Times investigation found The Weather Channel was just one of at least 75 companies getting purportedly "anonymous" but pinpoint-precise location data from about 200 million smartphones across the US. They're often sharing it or selling it to advertisers, retailers or even hedge funds that are seeking valuable insights into consumer behavior. As one example, a company known as "Tell All Digital" a Long Island based advertising firm, buys location data, then uses it to run ad campaigns for personal injury lawyers that it markets to people who wind up in emergency rooms.

The Times reviewed a database holding location data gathered in 2017 and held by one company, finding that it held "startling detail" about people's travels, accurate to within a few yards and in some cases updated more than 14,000 times a day. Several of the businesses whose practices were analyzed by the Times claim to track up to 200 million mobile devices in the US.

And… it's big business: Sales of location-targeted advertising reached an estimated $21 billion in 2018. But there's more to it than advertising: IBM got into the industry in 2015, when it purchased the digital side of TWC, with an eye to helping industries "operationalize their understanding of the impact of weather on business outcomes." (Whatever the heck THAT means.)

According to what Los Angeles City Attorney Michael N. Feuer told the Times, whatever's being done with our location data, including whether it's being sold to personal injury lawyers as we sit in the emergency room, we have a right to know about it. He was quoted as saying:

"If the price of getting a weather report is going to be the sacrifice of your most personal information about where you spend your time day and night, you sure as heck ought to be told clearly in advance."

And for their part, an IBM spokesman, Saswato Das, told the Times that TWC plans to fight the suit: *"The Weather Company has always been transparent with use of location data; the disclosures are fully appropriate, and we will defend them vigorously."*

The Ethereum blockchain is hit with an expensive "51%" attack
The rollback attack enabled attackers to re-spend 219,500 previously spent coins, valued at ~$1.1 million.

When this podcast first described the detailed operation of the Bitcoin blockchain we mentioned that one of the key assumptions, in fact, the cornerstone assumption for the security and trustworthiness of any blockchain-based technology, is a large community pool of honest participants who mutually concur and authenticate blockchain events.

Page 3 of Satoshi's original whitepaper titled: "Bitcoin: A Peer-to-Peer Electronic Cash System" states: "If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains."

Stated another way, the the blockchain to remain secure, no single actor must ever be able to obtain a majority of the chain's total processing power... because someone who is able to dominate the chain rules the chain... and is thus able to cheat others. And that's has been happening since January 5th to the Ethereum Classic blockchain.

At the expense of significant computation, attackers have been able to rewrite history. They rolled back and reorganized the Ethereum Classic blockchain and were thus able to "double spend" by recovering previously spent coins and transfer them to a new entity.

https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

Coinbase's Security Engineer, Mark Nesbitt, wrote in the Coinbase blog about these events:

"The function of mining is to add transactions to the universal, shared transaction history, known as the blockchain. This is done by producing blocks, which are bundles of transactions, and defining the canonical history of transactions as the longest chain of blocks. If a single miner has more resources than the entirety of the rest of the network, this miner could pick an arbitrary previous block from which to extend an alternative block history, eventually outpacing the block history produced by the rest of the network and defining a new canonical transaction history."*

Timeline:

- Late on the evening of Saturday 1/5, our systems alerted us to a deep reorg in ETC that contained a double spend. Our on-call engineers responded to the alert and worked to confirm the report through the night. We determined that we would temporarily halt send/receive interaction with the ETC blockchain in order to safeguard customer funds.

- This meant that customers who tried to send or receive ETC on Coinbase Consumer or Pro were unable to complete their transactions.

- On the morning of Sunday 1/6 we posted an update on status.coinbase.com stating (that) "Due to unstable network conditions on the Ethereum Classic network, we have temporarily disabled all sends and receives for ETC. Buy and sell is not impacted. All other systems are operating normally."

- We performed an analysis on Sunday afternoon/evening to confirm the pattern and determine the key details of the double-spend attacks. Beginning Sunday afternoon, we observed 8 more incidents, all containing double spends.

- Out of an abundance of caution, we did not put up a blog post prior to legal and technical review. A false alarm could have inadvertently caused market instability.

- On Monday 1/7 morning after legal and technical review, we finalized our public analysis and posted to our blog and social media accounts.

Today's status: https://status.coinbase.com/

Ethereum Classic: Under Maintenance.

A court recently rules that we needn't give law enforcement the finger -- or our finger.
https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/

Thomas Brewster, who is Forbes' cybersecurity reporter, yesterday ran a story with the headline: "Feds Can't Force You To Unlock Your iPhone With Finger Or Face, Judge Rules."

A California judge has ruled that American cops can't force people to unlock a mobile phone with their face or finger. The ruling goes further to protect people's private lives from government searches than any before and is being hailed as a potentially landmark decision.

Previously, U.S. judges had ruled that police were allowed to force unlock devices like Apple's iPhone with biometrics, such as fingerprints, faces or irises. That was despite the fact feds weren't permitted to force a suspect to divulge a passcode. But according to a ruling uncovered by Forbes, all logins are equal.

The order came from the U.S. District Court for the Northern District of California in the denial of a search warrant for an unspecified property in Oakland. The warrant was filed as part of an investigation into a Facebook extortion crime, in which a victim was asked to pay up or have an "embarassing" video of them publicly released. The cops had some suspects in mind and wanted to raid their property. In doing so, the feds also wanted to open up any phone on the premises via facial recognition, a fingerprint or an iris.

While the judge agreed that investigators had shown probable cause to search the property, they didn't have the right to open all devices inside by forcing unlocks with biometric features.

On the one hand, magistrate judge Kandis Westmore ruled the request was "overbroad" as it was "neither limited to a particular person nor a particular device."

But in a more significant part of the ruling, Judge Westmore declared that the government did not have the right, even with a warrant, to force suspects to incriminate themselves by unlocking their devices with their biological features. Previously, courts had decided biometric features, unlike passcodes, were not "testimonial." That was because a suspect would have to

willingly and verbally give up a passcode, which is not the case with biometrics. A password was therefore deemed testimony, but body parts were not, and so not granted Fifth Amendment protections against self-incrimination.

That created a paradox: How could a passcode be treated differently to a finger or face, when any of the three could be used to unlock a device and expose a user's private life?

And that's just what Westmore focused on in her ruling. Declaring that "technology is outpacing the law," the judge wrote that fingerprints and face scans were not the same as "physical evidence" when considered in a context where those body features would be used to unlock a phone.

The judge wrote: "If a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device. The undersigned finds that a biometric feature is analogous to the 20 nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial."

There were other ways the government could get access to relevant data in the Facebook extortion case "that do not trample on the Fifth Amendment," Westmore added. They could, for instance, ask Facebook to provide Messenger communications, she suggested. Facebook has been willing to hand over such messages in a significant number of previous cases Forbes has reviewed.

It feels that, ultimately, this will be another issue to be finally decided by the highest court in our land. I wonder what will happen in other countries?

Firefox 69 will FINALLY disable Adobe Flash plugin, by default.
... though not until September of this year.

The Flash plug-in is the last remaining NPAPI. The NPAPI is the "Netscape Plugin Application Programming Interface." Other than for use with FLASH, it is a deprecated API for browser extensions. It was first developed for Netscape browsers, starting in 1995 with Netscape Navigator 2.0, but was later adopted by other browsers. The developer.chrome.com site says of NPAPI: "NPAPI Plugin support for extension has been discontinued. The documentation below is preserved for historical purposes only.

Warning

NPAPI is a really big hammer that should only be used when no other approach will work.

Code running in an NPAPI plugin has the full permissions of the current user and is not sandboxed or shielded from malicious input by Google Chrome in any way. You should be especially cautious when processing input from untrusted sources, such as when working with content scripts or XMLHttpRequest.

Because of the additional security risks NPAPI poses to users, extensions that use it will require manual review before being accepted in the Chrome Web Store."

And this, of course, is why continued FLASH support is so inherently dangerous. It is not sandboxed because sandboxing didn't exist and was not needed back in 1995!

Once Flash has been disabled by default in Firefox, users will not be prompted to enable Flash, but they will be able to activate Flash on certain sites using browser settings. (If we MUST have it, that seems exactly right.) And then the final step for Flash on Firefox is due in early 2020 when Adobe officially "End of Life"s Flash and completely removes it from the consumer versions of Firefox. Flash will continue to be supported in the Firefox Extended Support Release (ESR) version until the end of 2020. In 2021 Firefox will "refuse to load the plugin".

Microsoft will also be disabling Flash by default in Edge and Internet Explorer in mid to late 2019.

And Google will be disabling Flash by default in Chrome 76, which is due for stable release around July. Chrome users will still be able to enable Flash in Settings, but the plugin will require explicit permission. As of Chrome 69, users need to give permission for each site to use Flash every time the browser is restarted. That's a nice deterrent, too.

I'm reminding everyone of this, because, aside from the security win of removing this longstanding security nightmare, whenever I mention this I receive notes from our knowledgeable listeners within various enterprises who are still seriously dependent upon this creaky old technology. And it is not its age that I have a problem with... it's that it has always been buggy as hell and Adobe never really cared to expend the time or energy to fix it. Its existence has hurt countless innocent Internet users and the sooner it dies the better.

So my point for those whose enterprises are still dependent upon Flash... the clock is ticking and those old Flash apps are going to need replacing this year.

Errata

MikeD: Subject -- "Steve ... it is promounced 'Gee-Drah'"

> Love SN, have been listening from the beginning. In terms of the current episode ...
>
> Clearly you are not spending enought time watching 'bad cinema' <chuckle> 'It' (Ghidrah, King Ghidra, King Ghidora and/or Monster Zerois) one of the 'Monsters' from the same 'linieage' of Japaneese 'monster movies' as Godzilla, Mothra and many others. 'It' appeares in several of 'those' movies and even takes on Godzilla in one <wink>

Miscellany

Windows 10's Disk Cleanup Getting a New Warning About Downloads Folder
https://www.bleepingcomputer.com/news/microsoft/windows-10s-disk-cleanup-getting-a-new-warning-about-downloads-folder/

Evan Katz: *"P.S. Yes, Filemail is amazing, and the best large-file transfer service that exists! I have used it for years. :)"*

Zerodium

https://zerodium.com/program.html

We are Zerodium

The leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities. "We pay BIG bounties, not bug bounties"

"Our Exploit Acquisition Program"

Program Overview

ZERODIUM is the leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities. **We pay BIG bounties to security researchers** to acquire their original and previously unreported zero-day research. While the majority of existing bug bounty programs accept almost any kind of vulnerabilities and PoCs but pay very low rewards, **at ZERODIUM we focus on high-risk vulnerabilities with fully functional exploits** and we pay the highest rewards (**up to $2,000,000 per submission**).

Eligible Research

ZERODIUM is currently acquiring zero-day exploits and innovative security research related to the following products:

Operating Systems

Remote code execution or local privilege escalation:
- Microsoft Windows 10/8.1/Servers
- Apple macOS Mojave / High Sierra
- Linux / BSD (CentOS/Ubuntu/etc)
- VM Escape (VMware ESXi or Wrks)

Web Browsers

Remote code execution, or sandbox bypass/escape, or both:
- Google Chrome
- Microsoft Edge
- Mozilla Firefox / Tor Browser
- Apple Safari

Clients / Files

Remote code execution or sensitive information disclosure:
- MS Office (Word/Excel/PowerPoint)
- PDF Readers (Adobe / Foxit)
- Email Clients (Outlook/Thunderbird)
- File Archivers (WinRAR/7-Zip/WinZip)

Mobiles / Smartphones

Remote code execution, or privilege escalation, or any other exploit type:
- Apple iOS 12.x
- Android 9.x / 8.x
- BlackBerry 10
- Windows 10 Mobile

Web Servers

Remote code execution or sensitive information disclosure:
- Apache HTTP Server
- Microsoft IIS Server
- nginx web server
- PHP / ASP
- OpenSSL / mod_ssl

Email Servers

Remote code execution or sensitive information disclosure:
- MS Exchange
- Dovecot
- Postfix
- Exim
- Sendmail

WebApps / Panels

Remote code execution, or SQL injection, or information disclosure:
- cPanel / Plesk / Webmin
- WordPress / Joomla / Drupal
- vBulletin / MyBB / phpBB
- IPS Suite / IP.Board
- Roundcube / Horde

Research / Techniques

Any other security research, exploit, or technique related to:
- WiFi / Baseband RCE
- Routers / IoT RCE
- AntiVirus RCE/LPE
- Tor De-anonymization
- Mitigations Bypass

Eligible Mobile Brands

Apple, Google, Samsung, LG, Huawei, Sony, HTC, Xiaomi, Acer, Asus, Vivo, Motorola, Lenovo, OPPO, BlackBerry, Vertu, ZTE, BBK, and Gionee.

Eligible Linux/BSD Distributions

CentOS, Fedora, Red Hat Enterprise Linux, Ubuntu, Debian, Tails, NetBSD, OpenBSD, and FreeBSD.

Eligible Router Brands

ASUS, Cisco, D-Link, Huawei, Linksys, MikroTik, Netgear, TP-Link, and Ubiquiti.

NOTE: If you have zero-day exploits for other products or systems not listed above, feel free to submit minimal details and we will be glad to discuss the opportunity.

New Payouts Highlights

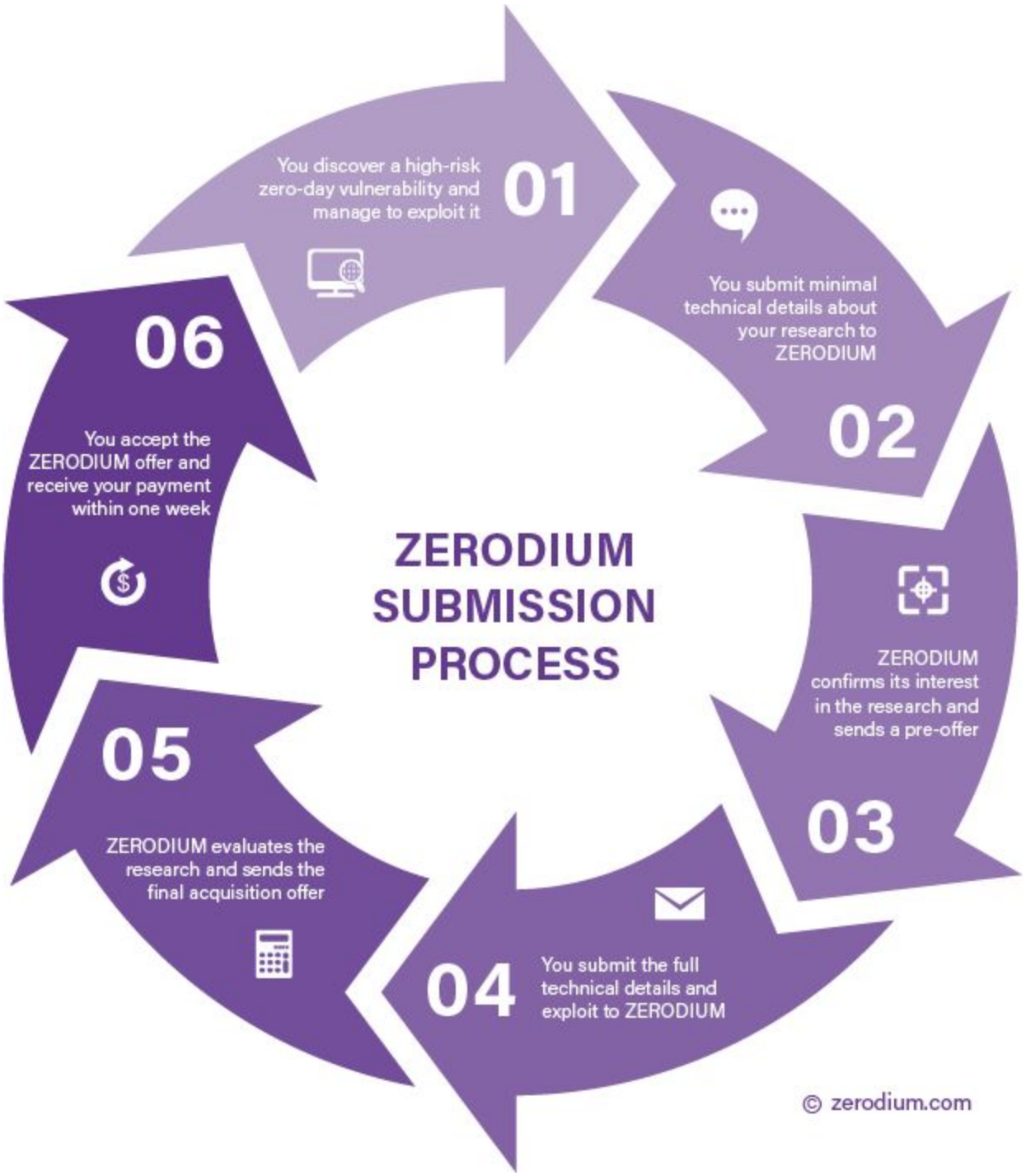
Jan. 7, 2019 - Payouts for the majority of Desktops/Servers and Mobile exploits have been increased. Major changes are highlighted below:

Modification	Details
Increased Payouts (**Mobiles**)	**$2,000,000** - Apple iOS remote jailbreak (Zero Click) with persistence (previously: **$1,500,000**) **$1,500,000** - Apple iOS remote jailbreak (One Click) with persistence (previously: **$1,000,000**) **$1,000,000** - WhatsApp, iMessage, or SMS/MMS remote code execution (previously: **$500,000**) **$500,000** - Chrome RCE + LPE (Android) including a sandbox escape (previously: **$200,000**) **$500,000** - Safari + LPE (iOS) including a sandbox escape (previously: **$200,000**) **$200,000** - Local privilege escalation to either kernel or root for Android or iOS (previously: **$100,000**) **$100,000** - Local pin/passcode or Touch ID bypass for Android or iOS (previously: **$15,000**) NOTE: Payouts were also increased for other products including: RCE via documents/medias, RCE via MitM, ASLR or kASLR bypass, information disclosure, etc.
Increased Payouts (**Servers/Desktops**)	**$1,000,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **$500,000**) **$500,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **$250,000**) **$500,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **$250,000**) **$250,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **$150,000**) **$250,000** - PHP or OpenSSL RCE (previously: **$150,000**) **$250,000** - MS Exchange Server RCE (previously: **$150,000**) **$200,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **$100,000**) **$80,000** - Windows local privilege escalation or sandbox escape (previously: **$50,000**) NOTE: Payouts were also increased for other products including: Thunderbird, VMWare Workstation, Plesk, cPanel, Webmin, WordPress, 7-Zip, WinRAR, etc.

ZERODIUM Payouts

ZERODIUM payouts for eligible zero-day exploits range from $2,000 to $2,000,000 per submission. The amounts paid by ZERODIUM to researchers to acquire their original zero-day exploits depend on the popularity and security level of the affected software/system, as well as the quality of the submitted exploit (full or partial chain, supported versions/systems/architectures, reliability, bypassed exploit mitigations, default vs. non-default components, process continuation, etc). For more information, please read our FAQ.

The payout ranges listed below are provided for information only and are intended for fully functional/reliable exploits meeting ZERODIUM's highest requirements. **ZERODIUM may pay even higher rewards for exceptional exploits and research**.



Sep. 19, 2018 - We are acquiring pre-authentication RCE **exploits affecting the following Routers**: ASUS, Cisco, D-Link, Linksys, MikroTik, Netgear, TP-Link, and Ubiquiti. Exploits leading to authentication bypass or credentials disclosure are also accepted. Exploits relying on XSS or CSRF are not eligible.

Dec. 20, 2018 - We are currently looking for **code execution exploits via USB drives** on Windows and/or macOS. The exploit must achieve code execution immediately after the USB key/drive is plugged into the system without relying on visible keystroke injections or user interaction.

https://zerodium.com/faq.html

How the acquired security research is used by ZERODIUM?

ZERODIUM extensively tests, analyzes, validates, and documents all acquired vulnerability research and reports it, along with protective measures and security recommendations, solely to its clients subscribing to the ZERODIUM Zero-Day Research Feed.

Who are ZERODIUM's customers?

ZERODIUM customers are mainly government organizations in need of specific and tailored cybersecurity capabilities and/or protective solutions to defend against zero-day attacks.

Access to ZERODIUM solutions and capabilities is highly restricted and is only available to a very limited number of organizations. ZERODIUM does not have any sales partner or reseller, our solutions are only available through our direct channel.

~30~