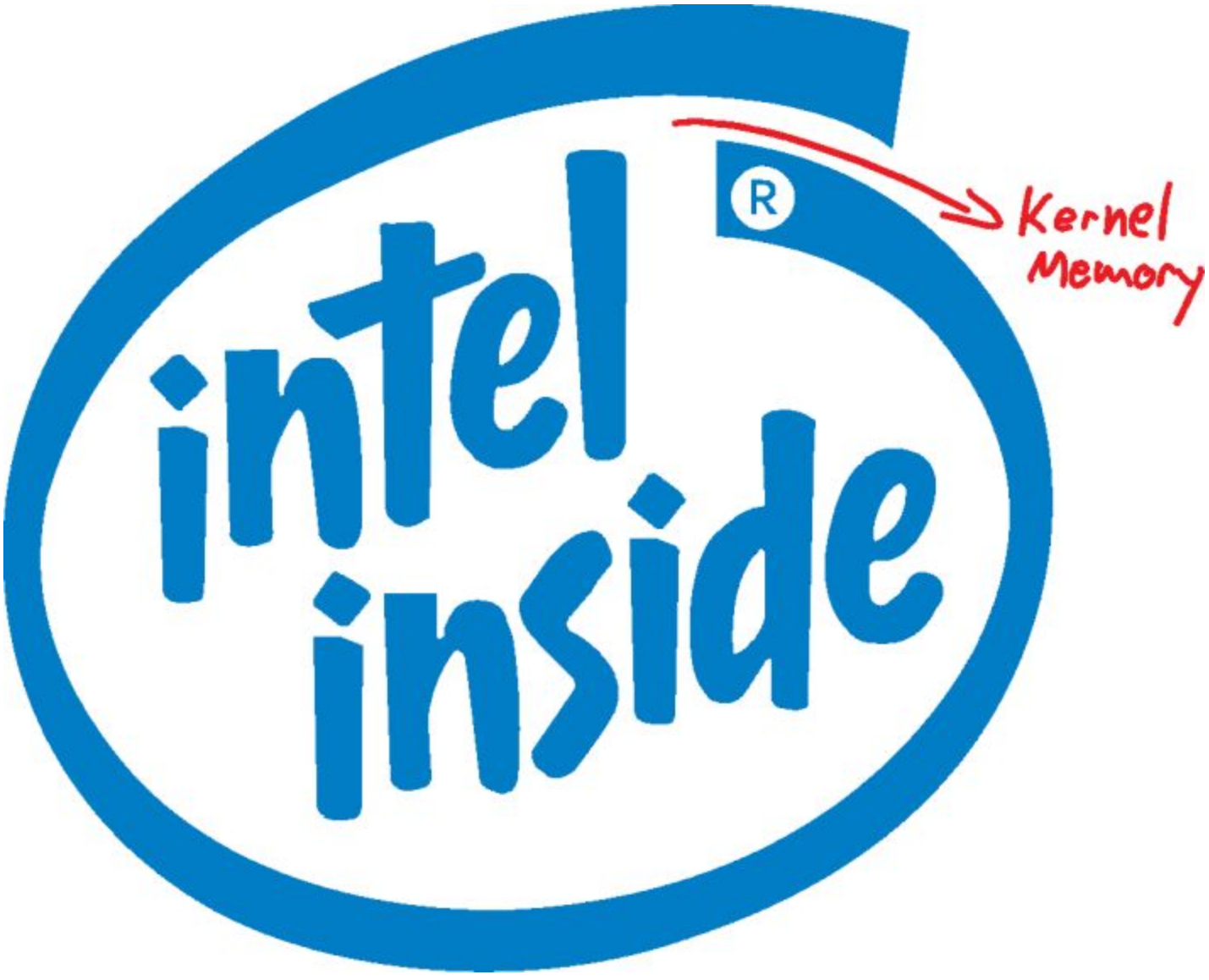
Security Now! #649 - 02-06-18

Meltdown & Spectre Emerge

This week on Security Now!

This week we observe that the Net Neutrality battle is actually FAR from lost, ComputerWorld's Woody Leonard enumerates a crazy January of updates, "EternalBlue" is turning out to be far more eternal than we'd wish, will Flash EVER die? A new 0-day Flash exploit in the wild, what happens when you combine Shodan with Metasploit?, Firefox 59 takes another privacy-enhancing step forward, a questionable means of sneaking data between systems, another fun SpinRite report from the field, some closing the loop feedback from our listeners, and a look at the early emergence of Meltdown and Spectre exploits appearing in the wild.



Security News

Net Neutrality is clearly far from dead.
In the wake of the FCC's removal of the 2015 Open Internet Order, the US's many individual states are moving to use their own governing authority and in some cases their purchasing power, to bring ISPs to heel.

Wyoming and New York have already signed new legislation into law.

As I mentioned just as last week's podcast was starting, one of California's two new net neutrality laws passed through its state Senate 21 to 12 and is now headed to the state Assembly.

And many other states from Rhode Island to Washington -- coast to coast -- are gearing up to follow suit.

And all this, despite the FCC's intention to pre-empt individual states from stepping in and protecting their own residents, which was also something lobbied for strongly by Verizon and Comcast.

In California, the San Francisco Chronicle writes:

> Both bills are meant to give California officials rules to force Internet service companies to adhere to the principles of net neutrality to continue doing business within the state. Those principles broadly guarantee the makers of websites and apps equal access to Internet consumers without excess charges or special fees for faster service. The FCC threw out national net neutrality rules enacted in 2015 by the Obama administration, saying they were unnecessary.

The de León bill would give the state the ability to enforce net neutrality rules under existing consumer protection and unfair business practice laws. The bill also would prohibit state agencies from buying Internet service from companies that did not observe net neutrality rules.

The bills are only part of a movement by state officials across the country to enact local net neutrality controls. This month, state Attorney General Xavier Becerra joined state attorneys general in 21 states and the District of Columbia in a lawsuit challenging the FCC repeal.

That state count is now up to 22 and counting. In reporting on this, TechDirt wrote:

> The legal fight over the FCC's historically unpopular decision to kill net neutrality has begun. An announcement by New York Attorney General Eric Schneiderman's office indicates that 22 State Attorneys General have filed suit against the FCC.
>
> The AGs says the multi-state coalition has filed a petition for review in the U.S. Court of Appeals for the D.C. Circuit, the first of what's expected to be numerous lawsuits in the weeks and months to come.
>
> The announcement makes it clear the suit intends to focus on the FCC's potential violation of the Administrative Procedure Act. Under the Act the FCC will need to prove that the

broadband market changed so substantially since the passage of the original rules in 2015 as to warrant such a stark reversal. Under the Act, a decision can be declared "arbitrary and capricious" if the regulator in question cannot prove such a dramatic change. And no such proof exists.

Not surprisingly, the folks at the EFF is on the case and Ernesto Falcon there posted their opinion that the California legislation which recently passed will be needlessly vulnerable to challenge in court. The way that first bill went about enforcing net neutrality subjects it to federal pre-emption. The EFF suggested to the CA lawmakers, who apparently ignored their advice, three powerful avenues of control:

- First: California spends $100s of millions on ISPs, including AT&T, as part of its California broadband subsidy program. The state could require that recipients of that funding provide a free and open Internet, to ensure that taxpayer funds are used to benefit California residents rather than subsidizing a discriminatory network. This is one of the strongest means the state has to promote network neutrality, and it is missing from SB 460.

- Second: California also has oversight and power over more than 4 million utility poles that ISPs benefit from accessing to deploy their networks. In fact, California is expressly empowered by federal law to regulate access to the poles and the state legislature can establish network neutrality conditions in exchange for access to the poles. Again, that is not in the current bill passed by the Senate.

- Third: Each city negotiates a franchise with the local cable company and often the company agrees to a set of conditions in exchange for access to valuable, taxpayer-funded rights of way. California's legislature can directly empower local communities to negotiate with ISPs to require network neutrality in exchange for the benefit of accessing tax-payer funded infrastructure. This is also not included in the current bill.

The bottom line appears to be that ultimately ISPs are on the losing end of this battle because, as the EFF demonstrates, ISPs are able to operate only with the permission of much more local authority. So long as the majority of US citizens want neutral access to Internet services -- and that fact is not in dispute -- we will be able to obtain them.

Woody on Windows:
Woody Leonard has been around a long time, and he is pretty much disgusted with January. The perfect end to a perfect month: Yet another Win10 1709 cumulative update, KB 4058258

(and, sure enough... it was waiting for me this morning.)

Today is the 15th day this month that we've seen Windows patches, yanked patches, patches of patches and re-re-re-patches. Welcome to the third cumulative update for Win10 Fall Creators Update this month.

https://www.computerworld.com/article/3252808/microsoft-windows/perfect-end-to-a-perfect-month-yet-another-win10-1709-cumulative-update-kb-4058258.html

Woody enumerates the January fiasco in detail. I won't go into it here since there's a link in the show notes for anyone who wants every painful detail. But, in short, Woodly notes that we received patches on January 3, 4, 8, 9, 11, 12, 17, 19, 22, 23, 24, 26, 29, 30, 31. And... remember that some of them you need to go get if you want them.

Cryptocurrency Mining Malware Infected Over Half-Million PCs Using NSA Exploit
https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html

EternalBlue is the Windows SMBv1 exploit, believed to have been developed by the NSA and leaked by the ShadowBrokers hacking group. It was leveraged by the widespread WannaCry ransomware which devistated the UK's NHS health system's network. EternalBlue was also used by the Petya/NonPetya worm.

Microsoft issued a security update to patch the flaw last March 14th, 2017... and in a surprising twist, Microsoft even patched the long-unsupported Windows XP for the same flaw.

At its peak, tens of thousands of machines were infected.

Now... fast forward to today, nearly one year later:

EternalBlue exploitation remains alive and well with several cybersecurity firms reporting the discovery of a new cryptocurrency mining viruse that's being spread using EternalBlue.

Researchers from Proofpoint discovered a massive global botnet dubbed "Smominru," a.k.a Ismo, that is using EternalBlu to spread and infect Windows computers to mine Monero cryptocurrency.

Active since at least May 2017 (so two months AFTER Microsoft issued the Windows SMBv1 patch), the Smominru botnet has infected more than 526,000 Windows computers, most of which are believed to be servers running unpatched versions of Windows, according to the researchers.

Based on the hash power associated with the Monero payment address for this operation the mining network is massive an the botnet has already mined approximately 8,900 Monero, valued at approximately $3.6 million USD and the mining is currently running at the rate of roughly 24 Monero per day ($8,500).

And while we're on the subject of oldies but goodies...
A new and currently unpatched Adobe Flash Player Zero-Day Exploit Spotted in the Wild
https://thehackernews.com/2018/02/flash-zero-day-exploit.html

South Korea spotted a Flash Player 0-day being used by North Korean hackers against South Koreans who research North Korea.

It's a "User After Free" Critical vulnerability capable of Remote Code Execution.

Adobe knows about this and has issued a security advisory
https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

> A critical vulnerability (CVE-2018-4878) exists in Adobe Flash Player 28.0.0.137 and earlier versions. Successful exploitation could potentially allow an attacker to take control of the affected system.
>
> Adobe is aware of a report that an exploit for CVE-2018-4878 exists in the wild, and is being used in limited, targeted attacks against Windows users. These attacks leverage Office documents with embedded malicious Flash content distributed via email.
>
> Adobe will address this vulnerability in a release planned for the week of February 5.

http://get.adobe.com/flashplayer/about/

Now at version 28.0.0.161 versions 28.0.0.137 and earlier are vulnerable.

You DEFINITELY want to be running a Flash Blocker on your web browser.

Recent version of Microsoft Office offer "Protected View" which notices when office documents are obtained online and raises its shields. File / Options / Trust Center / Trust Center Settings / Protected View.
[x] Enable Protected View for file originating from the Internet.
[x] Enable Protected View for file located in potentially unsafe locations.
[x] Enable Protected View for Outlook attachments.

What do you get when you combine the Shodan global search engine with the MetaSploit exploitation toolkit?
Aside from lots more trouble, you get "AutoSploit" -- now available on Github.

As its Pseudonymous author "Vector" states on Github:
As the name might suggest AutoSploit attempts to automate the exploitation of remote hosts. Targets are collected automatically as well by employing the Shodan.io API. The program allows the user to enter their platform specific search query such as; Apache, IIS, etc, upon which a list of candidates will be retrieved.

After this operation has been completed the 'Exploit' component of the program will go about the business of attempting to exploit these targets by running a series of Metasploit modules against them. Which Metasploit modules will be employed in this manner is determined by programmatically comparing the name of the module to the initial search query. However, I have added functionality to run all available modules against the targets in a 'Hail Mary' type of attack as well.

The available Metasploit modules have been selected to facilitate Remote Code Execution and to attempt to gain Reverse TCP Shells and/or Meterpreter sessions. Workspace, local host and local port for MSF facilitated back connections are configured through the dialog that comes up before the 'Exploit' component is started.

What is "Meterpreter" you ask? Ah...
As "Offensive Security" describes it:
Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

The Github presentation notes under "Operational Security Consideration"
Receiving back connections on your local machine might not be the best idea from an OPSEC standpoint. Instead consider running this tool from a VPS that has all the required dependencies available.

And, predictably, the wider security community is unhappy. Richard Bejtlich with TaoSecurity replied on Twitter in response to Vector's announcement:

"There is no need to release this. The tie to Shodan puts it over the edge. There is no legitimate reason to put mass exploitation of public systems within the reach of script kiddies. Just because you can do something doesn't make it wise to do so. This will end in tears."

Firefox continues to advance its users privacy.
Starting with Firefox 59, private browsing mode will strip the path information after the domain from Refer headers.

Referer:

Referer headers are already NOT sent with non-HTTPS requests from HTTPS pages or for "file" or "data" URI's.

Referer headers have historically allowed websites to determine where visitors are coming from, which has been quite useful. But the headers are also a privacy concern because they can leak data about the individual browsing. In one instance, researchers at the EFF (Electronic Frontier Foundation) found that referer headers from healthcare.gov were passing on data about the age and zip code of the user, along with whether they were a smoker or not, and their income.

(Who the hell designed that site?... this information would have had to have been in the originating page's URL tail!)

But our web browsers also send a referrer value when requesting other details like ads, or other social media snippets integrated in a modern website, which means these embedded content features also know exactly what page their visitors are viewing.

So... to prevent this type of data leakage, from Firefox 59, the private browsing option will remove path information from referrer values sent to third parties, effectively stripping out additional data and only leaving the web domain.

Users can also change their default referrer options in Firefox. These will override the browser's default referrer policy and override the site author's referrer policy, putting the users choice first.

https://wiki.mozilla.org/Security/Referrer
about:config
Search: referer

network.http.referer.trimmingPolicy
controls how much referrer to send regardless of origin
values:
0 = (default) send the full URL
1 = send the URL without its query string
2 = only send the origin

network.http.referer.XOriginTrimmingPolicy
controls how much referrer to send across origins values:
0 = (default) send the full URL
1 = send the URL without its query string
2 = only send the origin

network.http.referer.XOriginPolicy
controls whether or not to send a referrer across origins values:
0 = (default) send the referrer in all cases
1 = send a referrer only when the base domains are the same
2 = send a referrer only on same-origin

From the "Where there's a will there's a way" department:

Abusing X.509 Digital Certificates for Covert Data Exchange
Newly discovered hack would allow attackers to send data between two systems during TLS negotiation, researchers say.
https://www.darkreading.com/attacks-breaches/abusing-x509-digital-certificates-for-covert-data-exchange/d/d-id/1330984

DarkReading:

Researchers at Fidelis Cybersecurity have identified a new technique that attackers can potentially employ for covertly exchanging data using X.509 digital certificates.

The method builds on previous research involving the abuse of text fields in digital certificates to move data across a network. It takes advantage of the way digital certificates are exchanged during the initial TLS handshake, or the mutual authentication process that happens when two systems attempt to establish or resume a secure session with each other.

Jason Reaves, the principal threat research engineer at Fidelis: "Most other research involving using X.509 certificates for data transfer involves the use of text fields in the certificate such as 'Subject' or some of the other common fields such as 'notbefore' and 'notafter'." Researchers have previously shown how attackers might use these text fields to covertly send and receive data between systems.

"[Our] method is embedding data inside of a certificate extension. This means you can send data between two systems purely from the TLS negotiation."

Yeah... okay... except either the certificates are all going to be bogus, or each one needs to be individually signed by a CA that the recipient trusts.

SpinRite

From: Matej (Matt) Bokan
Subject: DJ Steve - SpinRite Gibson saves the concert

Hi Steve.

I'm not a music producer but I've got a friend who is making music on a Korg Synthesizer which cost many many kilo dollars. These "beasts" have had SSDs in them for a long time now. On the day of the concert there was a sound check, and this synth has all the rhythms, beats and whatnot of the band stored inside. But on that day, it wasn't working properly. Everything was having such a lag, or wouldn't load properly, that the concert was in danger and in the process of being canceled.

I had helped this man setup and connect his living room with projector, surround and PC in my youth. So I got a call to ask if I could somehow transfer the data to another identical synth if they could find one on short notice.

I didn't even know about Korg Synths having SSD's but when I found out I ran SpinRite and half an hour later the Synth was singing like a rockstar. The concert wasn't canceled at the last second, and thousands of concert goers sadly don't even know that Steve Gibson was true Rockstar that day.

./matt

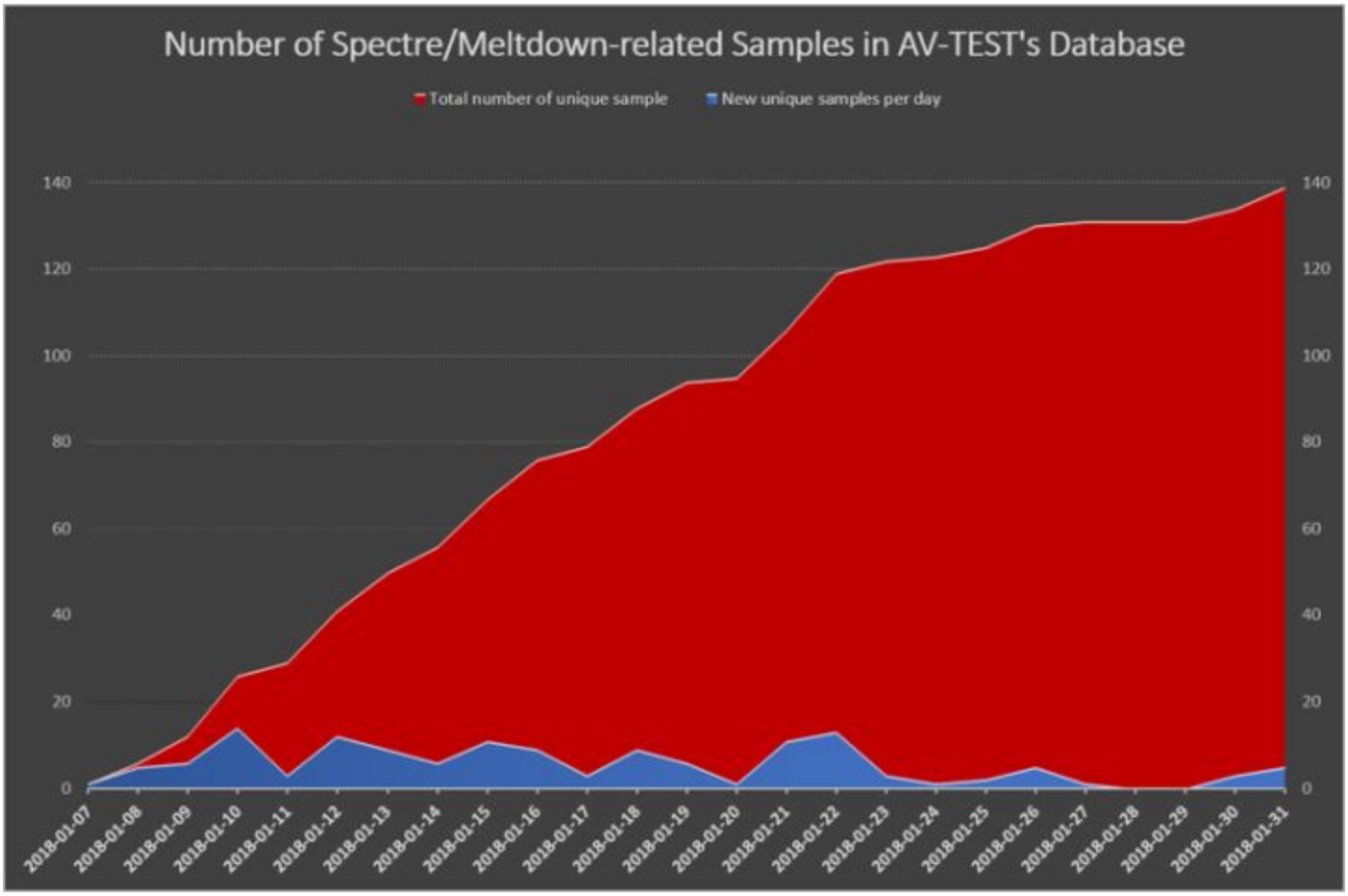
Closing The Loop

Chris Duncan (@cyberdunks)
@SGgrc Is it possible for @intel to encrypt and decrypt the on chip cache on the fly using its own keys as a mitigation for spectre? That way the chip knows what's in the cache for speculative execution and not the O/S.

Rob Fairhead (@raretrack)
Upgraded my network following the excellent Ubiquiti Home Network project at github.com/mjp66/Ubiquiti -first seen on @SGgrc #SecurityNow now have segregation for IoT devvices & guest network. Longtime itch scratched! (raretrack.uk/2018/02/204/)

Mike Potts - 105-page PDF:
https://github.com/mjp66/Ubiquiti/blob/master/Ubiquiti%20Home%20Network.pdf
Recently added support for the Quad9 DNS provider.

Meltdown & Spectre Appear



AV-TEST is an independent organization which evaluates and rates antivirus and security suite software for Microsoft Windows and Android operating systems under a variety of criteria.

By January 17, AV-TEST reported that it had seen 77 separate malware samples related to the CPU vulnerabilities.

That number had increased to 119 by January 23.

And by last Wednesday, AV-TEST had collected a total of 139 samples from various sources, including researchers, testers and antivirus companies.

Proof of Concept browser exploitation code for IE Chrome and Firefox now exists.

There is little innovation evident so far, but Malware authors are clearly focused upon the exploitation of these newly discovered and disclosed vulnerabilities.