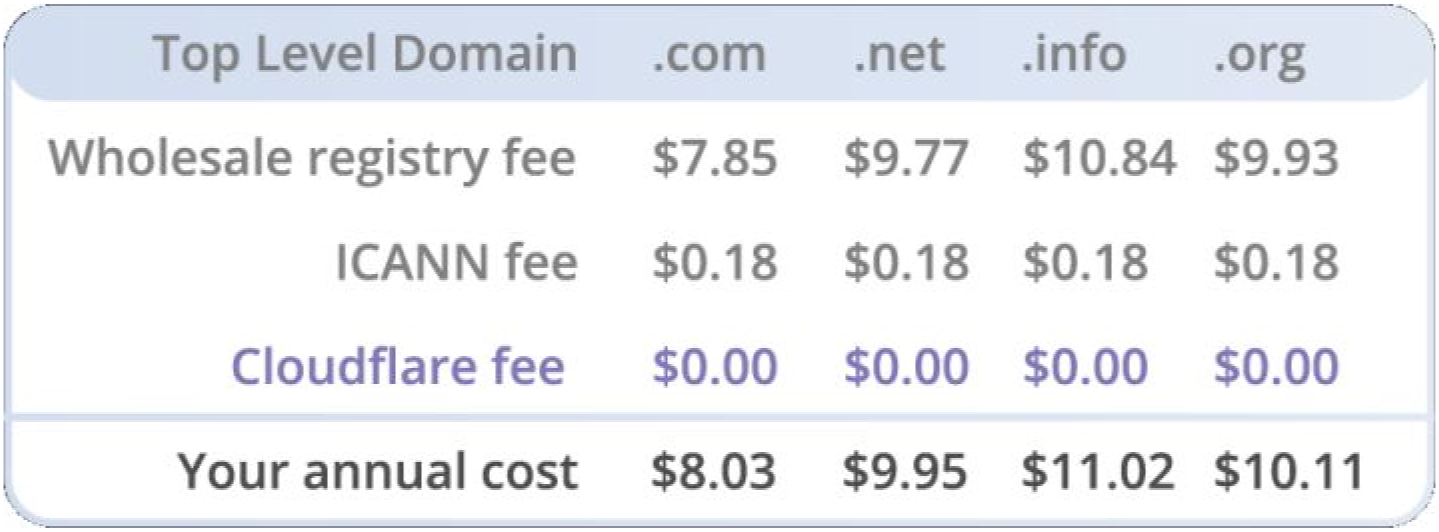
Security Now! #683 - 10-02-18

The Facebook Breach

This week on Security Now!

This week we discuss yet another treat from Cloudflare, the growing legislative battle over Net Neutrality, the rise of Python malware, Cisco's update report on the VPNFilter malware, still more Chrome controversy and some placating, the rapid exploitation of 0-day vulnerabilities, the first UEFI rootkit found in the wild, another new Botnet discovery, the danger of the RDP protocol, a nasty website browser trick, and how to thwart it, an quick update on recent non-fiction and science fiction, and then a look into the recent massive 50 million account Facebook security breach.

Cloudflare offers domains to its users at cost:



Top Level Domain	.com	.net	.info	.org
Wholesale registry fee	$7.85	$9.77	$10.84	$9.93
ICANN fee	$0.18	$0.18	$0.18	$0.18
Cloudflare fee	$0.00	$0.00	$0.00	$0.00
Your annual cost	$8.03	$9.95	$11.02	$10.11

Security News

Cloudflare adds domain registry services -- at cost:
https://blog.cloudflare.com/using-cloudflare-registrar/
https://www.cloudflare.com/products/registrar/

Cloudflare continues to make their offerings look better and better. They are a frequent topic of this podcast because of their leading edge security implementations. They are clearly always asking themselves the question "how can we make our services better?" and they often answer with significant security and privacy improvements.

In this instance I just wanted to add to their pile of goodness that they are now opening their previous limited domain registration to all customers. It had been previously for their enterprise clients. Now it's available and "at cost" for everyone. It's a smart move:

In a posting Thursday, Cloudflare wrote:

Every website, large or small, started with an idea, rapidly followed by registering a domain. Most registrars offer promotions for your initial domain registration and then quietly hike the price with each renewal. What they don’t tell customers is that the price they pay to a registry, for your registration, is set by the registry. In some cases, we’ve found registrars charging eight times the wholesale price for a domain renewal.

Today, we’re launching Cloudflare Registrar, the first domain registrar you can love. Cloudflare Registrar will never charge you more than what we pay to the registry for your domain. No markup and no surprise fees. For eight years Cloudflare has built products that make the internet faster and safer. It's time for us to start where your internet journey starts, your domain.

Cloudflare also blinds the WHOIS by default, which is nice since WHOIS spam is a thing and paying extra for WHOIS privacy (not to mention domain transfer protection), which Network Solutions and many other still do, is really annoying.

Network Solutions: "Free" † This offer provides Customer with private registration at no cost for the first billing cycle. Subsequent billing cycles will be billed at $1.99 per month (currently every 4 weeks). Customer may cancel prior to the end of the promotional period or at any time thereafter by contacting Network Solutions at 888-642-0209.

Just as I left Symantec/Verisign for DigiCert, I also left Network Solutions for Hover, and I've never looked back. (Except to transfer more domains away from Network Solutions. Today I only have two domains that I cannot Network Solutions was $35/year for a .com Hover is $15/year.

California, U.S. Government Battle Over Net Neutrality State Law
https://threatpost.com/california-u-s-government-battle-over-net-neutrality-state-law/137820/

The US DoJ filed a lawsuit against California (the 5th largest economy in the world) after California's Senate Bill "SB 822" passed on Sunday, which enforces net neutrality regulations on internet service providers.

The bill prevents internet providers from blocking, throttling or discriminating against any Internet content. The rules are similar to the previous Open Internet Order legislation which was passed in 2015, then repealed last December amid a great deal of controversy.

California's new legislation contains other features that make it an even stronger law around net neutrality than the former FCC approach, including prohibiting "zero rating," which would enable carriers to control which types of content would count towards a customers' data usage – including their own streaming services or content.

But upon its signing by state governor Jerry Brown, the DoJ responded with a lawsuit alleging that its regulations are unlawful. FCC Chairman, Ajit Pai said "I'm pleased the Department of Justice has filed this suit. The internet is inherently an interstate information service. As such, only the federal government can set policy in this area. And the U.S. Court of Appeals for the Eighth Circuit recently reaffirmed that state regulation of information services is preempted by federal law."

But Katharine Trendacosta, who is a policy analyst at the Electronic Frontier Foundation, argues that the law was written to be within state power: "The argument that the FCC preempted states acting to protect the net neutrality within their borders doesn't hold a lot of water when the FCC gave up jurisdiction of this area in the so-called 'Restoring Internet Freedom Order. You can't throw up your hands, walk away and say it's not your problem anymore, only to also say no one else can rush in to solve that problem. You gave up that right when you walked away."

It's worth noting, also, that California is far from alone in taking independent legislative action. The National Conference of State Legislatures indicates that 30 states have introduced over 72 bills requiring internet service providers to ensure and adhere to various net neutrality principles. And so far, governors of six states – including Hawaii, New Jersey, New York and Vermont – have signed executive orders around net neutrality, while three other states (Oregon, Vermont and Washington) have enacted net-neutrality legislation.

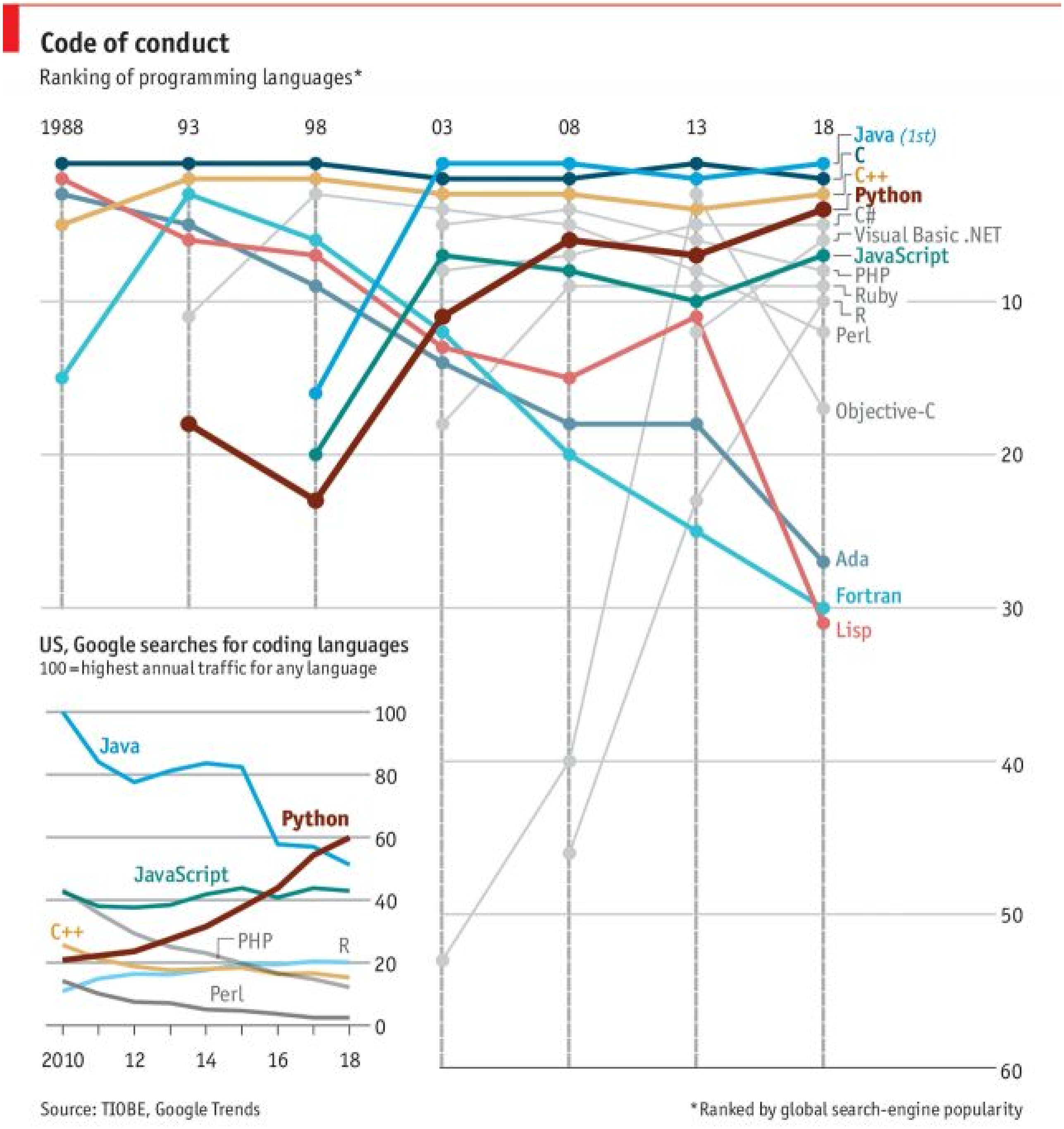
ThreatList: Hackers Turn to Python as Attack Coding Language of Choice
https://threatpost.com/threatlist-hackers-turn-to-python-as-attack-coding-language-of-choice/137757/

Python is growing to become the all-purpose coding language of choice, and one of those purposes, for better... or mostly for worse... is malware.

Today, more than 1 out of every 5 GitHub repositories containing an attack tool or proof of concept for an exploit are written in Python.

And not just on GitHub: This summer, between the end of June and mid-September, Python-based tools were used in up to 77 percent of attacks against sites seen in telemetry from Imperva.

And, from our recent reporting on and tracking of malware we know why: It's because malware is now rapidly expanding to become both broadly multi-platform and widely multi-exploit.



Code of conduct

Ranking of programming languages*

Source: TIOBE, Google Trends

*Ranked by global search-engine popularity

The Economist

Cisco concludes their sobering analysis of VPNFilter.
And speaking of growing IoT threats, recall our coverage of VPNFilter toward the end of May, after Cisco's Talos group discovered more than 500,000 diverse routers from Linksys, MicroTik, Netgear, TP-Link. At that time, Cisco said that they had not yet completed their research, but that they felt they needed to come forward and alert the public to what they had found so far.

https://blog.talosintelligence.com/2018/05/VPNFilter.html

A month later, in June, Cisco updated their initial report adding routers from ASUS, D-Link, Huawei, Ubiquiti, UPVEL and ZTE, with the total number of router models targeted by VPNFilter adversaries raised to 75.

(This was the malware that had a multi-stage deployment, set itself up in directories with "VPNFilter" in the path to hide in plain sight, and pulled its second-stage either from Photobucket or from the domain "toknowall.com" Then, from the image downloaded, the malware extracts an IP for the command and control server it will connect to from the EXIF image metadata.)

And perhaps most disturbing is that researchers are quite sure that a major state actor is behind VPNFilter.

So, now, last Wednesday, Cisco's Talos group has provided another update...

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

Paraphrasing from their updated report:

VPNFilter — a multi-stage, modular framework that has infected hundreds of thousands of network devices across the globe — is now known to possess even greater capabilities. Cisco Talos recently discovered seven additional third-stage VPNFilter modules that add significant functionality to the malware, including an expanded ability to exploit endpoint devices from footholds on compromised network devices. The new functions also include data filtering and multiple encrypted tunneling capabilities to mask command and control (C2) and data exfiltration traffic.

Talos has been researching VPNFilter for months. As part of our continued investigation, we developed a technique to examine a key protocol used by MikroTik networking devices to hunt for possible exploitation methods used by the actor.

As we followed the thread of VPNFilter infections, it became clear that MikroTik network devices were heavily targeted by the threat actor, especially in Ukraine. Since these devices seemed to be critical to the actor's operational goals, this led us to try to understand how they were being exploited. Part of our investigation included the study of the protocol used by MikroTik's Winbox administration utility.

The sophistication of VPNFilter drives home the point that this is a framework that all individuals and organizations should be tracking. Only an advanced and organized defense can combat these kinds of threats, and at the scale that VPNFilter is at, we cannot afford to overlook these new discoveries.

Expanded VPNFilter capabilities

The discovery of these additional VPNFilter third-stage modules has significantly added to our understanding of what we already knew to be an extremely potent threat. Together, these modules added:

- Additional capabilities that could be leveraged to map networks and exploit endpoint systems that are connected to devices compromised by VPNFilter.
- Multiple ways for the threat actor to obfuscate and/or encrypt malicious traffic, including communications used for C2 and data exfiltration.
- Multiple tools that could be utilized to identify additional victims accessible from the actor's foothold on devices compromised by VPNFilter for both lateral movement within a network, as well as to identify new edge devices in other networks of interest to the actor.
- The capacity to build a distributed network of proxies that could be leveraged in future unrelated attacks to provide a means of obfuscating the true source of attack traffic by making it appear as if the attacks originated from devices previously compromised by VPNFilter.

We were able to confirm the existence and capabilities of the malware after reverse-engineering these additional modules. Previously, we had to make analytic assessments on the existence and nature of these capabilities based solely on telemetry analysis, which always leaves room for error.

For example, we had previously noted what appeared to be devices compromised by VPNFilter conducting scans of large IP spaces that seemed focused on identifying other devices vulnerable to the methods of exploitation used by the actor associated with the VPNFilter malware. However, now we can discuss the specific third-stage module used for this activity.

As a result of our continued research, we have furthered our understanding of the full scope of the capabilities associated with VPNFilter after examining these additional third-stage modules.

Talos has identified the following seven additional third-stage modules that greatly expanded the capabilities present within VPNFilter:

"htpx" - Redirects and inspects the contents of HTTP traffic transmitted through the devices.

"ndbr" - A multifunctional SSH utility.

"nm" - Allows network mapping activities to be conducted from compromised devices.

"netfilter" - Denial of Service utility.

"portforwarding" - Allows the forwarding of network traffic to attacker-specified infrastructure.

"socks5proxy" - Enables the establishment of a SOCKS5 proxy on compromised devices.

"tcpvpn" - Enables the establishment of a reverse-TCP VPN on compromised devices.

Cisco's sobering conclusion:

As a result of the capabilities we previously discovered in VPNFilter coupled with our new findings, we now confirm that VPNFilter provides attackers all of the functionality required to leverage compromised network and storage devices to further pivot into and attack systems within the network environments that are being targeted.

It also allows attackers to leverage their access to sensitive systems such as gateway and routing devices to perform activities such as network mapping and endpoint exploitation, network communications monitoring and traffic manipulation, among other serious threats. Another dangerous capability provided by VPNFilter is the ability to turn compromised devices into proxies that could be leveraged to obfuscate the source of future, unrelated attacks by making it appear as if the attacks originate from networks previously compromised by VPNFilter. The sophisticated nature of this framework further illustrates the advanced capabilities of the threat actors making use of it, as well as the need for organizations to deploy robust defensive architectures to combat threats such as VPNFilter.

Yet another recent Chrome controversey

https://www.bleepingcomputer.com/news/google/chrome-69-keeps-googles-cookies-after-you-clear-browser-data/

Last week, Christoph Tavan noticed something about Chrome that Google clearly knew, deliberately chose to do, and even documented... but in this current "everyone pile on Chrome" environment it went over less well than it might have normally.

Christoph observed and tweeted that after he instructed Chrome to delete =ALL= of the cookies his Chrome browser had collected, it did that... except for Google's own cookies... which remained.

Under "Settings / Advanced / Clear browsing data" we're shown the number of things and amount of space being consumed by various browsing history, including, of course, the accumulated cookies. On the detail for "Cookies and other site data" Chrome clearly states parenthetically "(you won't be signed out of your Google Account)"

We know that cookies are the mechanism browsers use to maintain "state" with the sites they visit. So, "not being signed out of your Google Account" means that Google's cookies will not be removed from the browser.

Based upon the uproar caused by this misunderstanding, what Google should apparently have offered was a checkbox underneath the cookie report for "Also delete Google's own cookies and sign out of all Google accounts and services."

... which leads us into Google's comprehensive posting reply:

Product updates based on your feedback
https://www.blog.google/products/chrome/product-updates-based-your-feedback/

Anyone can make a mistake. What matters is that Google/Chromium is listening...

Last Wednesday: "Product updates based on your feedback" by Zach Koch, Chrome's Product Manager

(Zach first catches us up on recent events), then...

Over the years, we've received feedback from users on shared devices that they were confused about Chrome's sign-in state. We think these UI changes help prevent users from inadvertently performing searches or navigating to websites that could be saved to a different user's synced account.

We've heard—and appreciate—your feedback. We're going to make a few updates in the next release of Chrome (Version 70, released mid-October) to better communicate our changes and offer more control over the experience.

While we think sign-in consistency will help many of our users, we're adding a control that allows users to turn off linking web-based sign-in with browser-based sign-in—that way users have more control over their experience. For users that disable this feature, signing into a Google website will not sign them into Chrome.

We're updating our UIs to better communicate a user's sync state. We want to be clearer about your sign-in state and whether or not you're syncing data to your Google Account.

We're also going to change the way we handle the clearing of auth cookies. In the current version of Chrome, we keep the Google auth cookies to allow you to stay signed in after cookies are cleared. We will change this behavior that so all cookies are deleted and you will be signed out.

We deeply appreciate all of the passionate users who have engaged with us on this. Chrome is a diverse, worldwide community, and we're lucky to have users who care as much as you do. Keep the feedback coming.

GandCrab v5 Ransomware Utilizing the ALPC Task Scheduler Exploit
https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/

As predicted, malware was quick to jump onto the 0-day ALPC privilege elevation bug, leveraged through Windows Task Scheduler that existed briefly until it was patched in September's Windows update. Bleeping Computer reported that the GandCrab v5 Ransomware has started leveraging that vulnerability to gain full System privileges to more deeply infect a victim's PC.

The vulnerability is patched now, but it's worth nothing that this is the world we live in today: Bad guys know that disclosed vulnerabilities will have a very brief shelf life -- at least where updates are flowing and are being installed continuously (which is to say, not necessarily for 3rd-party packages such as Apache Struts, etc.). So they jump on them quickly to get whatever they can for their brief life.

In this environment, there's no way to view that public disclosure of this 0-day vulnerability as anything short of irresponsible.

ESET uncovers the first UEFI rootkit found in the wild.
https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf
(24-page PDF)

It comes courtesy of "Sednit", also known as APT28, Sofacy, Strontium, Fancy Bear, etc. (We really do all just need to choose and settle on just one name for this group!)

The rootkit is part of a malware system known as "LoJax" and the fact that it's from this group is what's mostly raising alarm bells... since this state-sponsored actor is big time serious.

The UEFI rootkit module has the responsibility of dropping the LoJax infection module onto the system. And since it's UEFI firmware based, it survives not only whole system wipe and restore, and also storage drive changes.

The various components which attempt to install the rootkit by writing to the system's firmware are common repurposed utility components which ARE signed. However, since the UEFI firmware itself is NOT signed, Secure Boot =will= prevent the execution of the rootkit malware and =only= systems without Secure Boot, or with Secure Boot disabled will be vulnerable to this attack.

New Iot Botnet Torii Uses Six Methods for Persistence, Has No Clear Purpose
https://blog.avast.com/new-torii-botnet-threat-research

The one thing the world definitely does not need is yet another Botnet, yet we have just that.

Dubbed "Torii" because it attacks device's Telnet ports through the TOR network, this previously unknown Botnet appears to have some heavy weight behind it.

It is superior to the seemingly endless Mirai variants which come and go because they lack a persistence mechanism. By contrast, Torii appears to be all about persistence. It boasts six different means for making sure that it survives reboots...

As Avast writes about Torii... the malware's dropper makes sure that the second stage payload is executed and that it will remain persistent. It is unique in that it is remarkably thorough in how it achieves persistence. It uses at least six methods to make sure the file remains on the device and always runs. And, not just one method is executed – it runs all of them.

- Automatic execution via injected code into ~\.bashrc
- Automatic execution via “@reboot” clause in crontab
- Automatic execution as a “System Daemon” service via systemd
- Automatic execution via /etc/init and PATH. Once again, it calls itself "System Daemon"
- Automatic execution via modification of the SELinux Policy Management
- Automatic execution via /etc/inittab

Avast says: The infection chain starts with a telnet attack on the weak credentials of targeted devices followed by execution of an initial shell script. This script looks quite different from typical scripts that IoT malware uses in that it is far more sophisticated.

The script initially tries to discover the architecture of the targeted device and then attempts to download the appropriate payload for that device.The list of architectures that Torii supports is quite impressive: including devices based on x86_64, x86, ARM, MIPS, Motorola 68k, SuperH, PPC - with various bit-width and endianness. This allows Torii to infect a wide range of devices running on these very common architectures.

Torii is written in 'GO' allowing it to be readily cross-compiled for any supported processor architecture. It's clear that the developers of the botnet are seeking broad coverage so they have built binaries for all popular CPU architectures, tailoring the malware for stealth and persistence. Communication with the command and control (C2) servers is encrypted and capabilities include exfiltration and, command execution.

AVAST concludes with...

Even though our investigation is continuing, it is clear that Torii is an example of the evolution of IoT malware, and that its sophistication is a level above anything we have seen before. Once it infects a device, not only does it send quite a lot of information about the machine it resides on to the CnC, but by communicating with the CnC, it allows Torii authors to execute any code or deliver any payload to the infected device. This suggests that Torii could become a modular platform for future use. Also, because the payload itself is not scanning for other potential targets, it is quite stealthy on the network layer.

Stay tuned for the follow ups.

Avast has provided a very comprehensive teardown of the malware for anyone who is interested. I've included their link in the show notes.

“Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity”
https://www.ic3.gov/media/2018/180927.aspx

Last Thursday... Not exactly a news flash, but still really really important.

To make their point, they provide four examples:

1. CrySiS Ransomware: CrySIS ransomware primarily targets US businesses through open RDP ports, using both brute-force and dictionary attacks to gain unauthorized remote access. CrySiS then drops its ransomware onto the device and executes it. The threat actors demand payment in Bitcoin in exchange for a decryption key.

2. CryptON Ransomware: CryptON ransomware utilizes brute-force attacks to gain access to RDP sessions, then allows a threat actor to manually execute malicious programs on the compromised machine. Cyber actors typically request Bitcoin in exchange for decryption directions.

3. Samsam Ransomware: Samsam ransomware uses a wide range of exploits, including ones attacking RDP-enabled machines, to perform brute-force attacks. In July 2018, Samsam threat actors used a brute-force attack on RDP login credentials to infiltrate a healthcare company. The ransomware was able to encrypt thousands of machines before detection.

4. Dark Web Exchange: Threat actors buy and sell stolen RDP login credentials on the Dark Web. The value of credentials is determined by the location of the compromised machine, software utilized in the session, and any additional attributes that increase the usability of the stolen resources.

VULNERABILITIES

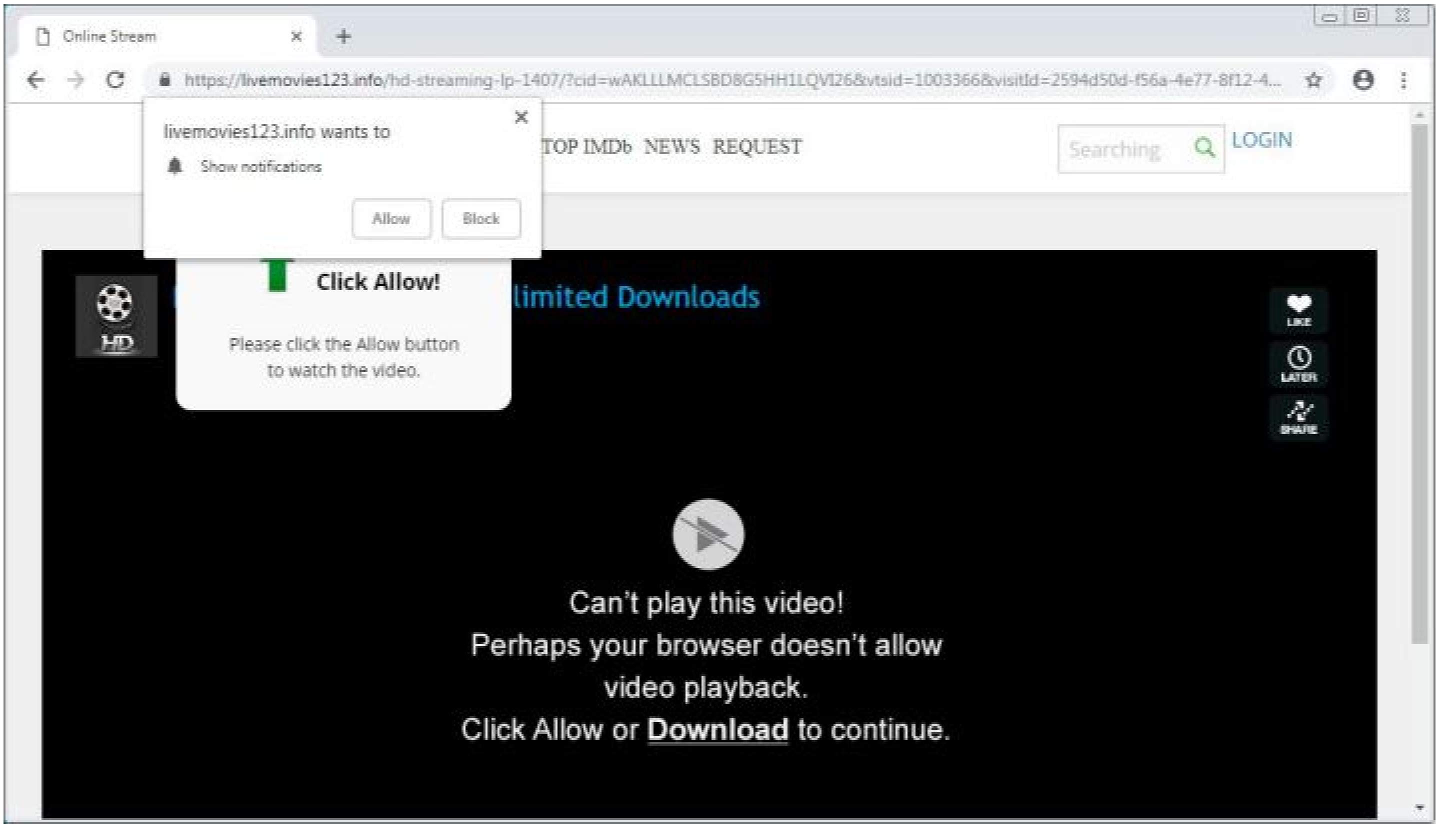
- Weak passwords – passwords using dictionary words or do not include a mixture of uppercase/lowercase letters, numbers, and special characters – are vulnerable to brute-force attacks and dictionary attacks.

- Outdated versions of RDP may use flawed CredSSP, the encryption mechanism, thus enabling a potential man-in-the-middle attack.

- Allowing unrestricted access to the default RDP port (TCP 3389).

- Allowing unlimited login attempts to a user account.

Sites Trick Users Into Subscribing to Browser Notification Spam
https://www.bleepingcomputer.com/news/security/sites-trick-users-into-subscribing-to-browser-notification-spam/


Online Stream
https://livemovies123.info/hd-streaming-lp-1407/?cid=wAKLLLMCLSBD8G5HH1LQVI26&vtsid=1003366&visitId=2594d50d-f56a-4e77-8f12-4...
TOP IMDb NEWS REQUEST
Searching
LOGIN
Allow
Block
HD
limited Downloads
LIKE
LATER
SHARE

livemovies123.info wants to

Show notifications

Click Allow!

Please click the Allow button to watch the video.

Can't play this video!
Perhaps your browser doesn't allow video playback.
Click Allow or **Download** to continue.

I have often been prompted by sites I visit asking permission to send me notices. What?!?

But apparently this allows our web browsers to create pop-up notifications ANYTIME on our desktop's notification area. And we =KNOW= that almost any site asking for this use and abuse this to annoy and harass us.

Get your popcorn ready for tomorrow's first-ever Presidential Alert.
(A lawsuit has been filed by three individuals who oppose the idea but it seems unlikely to gain any traction.)

REMINDER: Wednesday, 03 October 2018 Presidential Alert National Test 2:18 PM (EDT) - Wireless Emergency Alerts 2:20 PM (EDT) - Emergency Alert System (30-min duration) Department of Homeland Security Federal Emergency Management Agency Integrated Public Alert & Warning System

Miscellany

"Masters of Doom"
John Carmack and John Romero

The Rho Agenda

- The Second Ship
- Immune
- Workhole

The Rho Agenda Inception (the backstory about Jack and Janet)

- Once Dead
- Dead Wrong
- Dead Shift

The Rho Agenda Assimilation

- The Kasari Nexus
- The Altreian Enigma
- The Meridian Ascent

The Frontiers Saga

- 1-15
- 1-8...

"Salvation" -- Peter F. Hamilton.

Another completely new mega trilogy.

The "Salvation Sequence"

In the year 2204, humanity is expanding into the wider galaxy in leaps and bounds. Cutting-edge technology of linked jump gates has rendered most forms of transportation—including starships—virtually obsolete. Every place on Earth, every distant planet humankind has settled, is now merely a step away from any other. All seems wonderful—until a crashed alien spaceship of unknown origin is found on a newly located world eighty-nine light-years from Earth, carrying a cargo as strange as it is horrifying. To assess the potential of the threat, a high-powered team is dispatched to investigate. But one of them may not be all they seem. . . .

Bursting with tension and big ideas, Peter F. Hamilton’s Salvation is the first book of an all-new series that highlights the inventiveness of an author at the top of his game.

SpinRite

Facebook Breached

Matt Blaze (@mattblaze) / 5:30 PM - Sep 28, 2018
[CV:] Matt Blaze is a researcher in the areas of secure systems, cryptography, and trust management. He is an Associate Professor of Computer and Information Science at the University of Pennsylvania, and on the board of directors of the Tor Project.

<quote> We're seeing the flip side of concentrating authentication into a few giants like Facebook, Google, etc. They almost certainly DO do a better job securing sensitive data than a zillion small sites would. But when they get breached, it's a catatrasophe of ecological proportion.

Facebook Vulnerability Affecting 50 Million Users Allowed Account Takeover
https://www.bleepingcomputer.com/news/security/facebook-vulnerability-affecting-50-million-users-allowed-account-takeover/

Facebook Data Breach Impacts Almost 50 Million Accounts
https://threatpost.com/facebook-data-breach-impacts-almost-50-million-accounts/137801/

Check your Facebook login history to make sure no one has accessed your account from an unknown location or device.

OAuth “Login with Facebook” was also inherently vulnerable. Later Friday, Facebook confirmed that third-party sites that those users logged into with their Facebook accounts could also be affected.

WIRED: “Facebook initially responded by logging out both the 50 million people it knows were affected by the attack, and an additional 40 million who were looked up with the “View As” tool in the last year. It also hit pause on the “View As” feature. But the second revelation Friday indicates that the fallout may be far more widespread than initially indicated.

Beyond the impact on Facebook accounts themselves, the company confirmed that breach impacted Facebook's implementation of Single Sign-On, the practice that lets you use one account to log into others. The idea is to use a trusted service—like Facebook Google, Twitter, and so on—to log into sites and services across the web, rather than create a unique profile for each one. That saves time, and ensures you're logging in through an entity you trust. In this case, it also appears to have potentially made Facebook's breach an internet-wide calamity, at least for those impacted.

"The access token enables someone to use the account as if they were the account holder themselves. This does mean they could access other third-party apps using Facebook login," Guy Rosen, Facebook's vice president of product, said in a call with reporters Friday. "Developers who used Facebook login will be able to detect those access tokens have been reset."