Security Now! #819 - 05-18-21

The WiFi Frag Attacks

This week on Security Now!

This week we follow-up on last week's "News from the Darkside" with a surprising amount of happenings including the dark web's rejection of further ransomware. We look at blockchain analytics which are used to follow the dark money, the mixed signals now coming from the Darkside group and a live list of more than 2000 ransomware attacks during the past two years from the dark web. We cover last week's Patch Tuesday that you won't want to miss. We have a bit of miscellany, including the "Unidentified Aerial Phenomena Task Force" which is actually a thing, and some closing-the-loop feedback from our listeners regarding last week's Andy Weir's "Hail Mary" book mention. Then we take a close look at the biggest non-Colonial Pipeline news from last week: a new round of research which revealed a range of attacks on WiFi's security.

How NOT to store your cryptocurrency…

Darkside Follow-Up

The team at FireEye — eight members put their names on this — have done some deep and delicious research into the DarkSide group. They originally took this work public last Tuesday the 11th. But after news of the apparent DarkSide takedown surfaced, they updated their post last Friday to add the following preface:

> *Update (May 14): Mandiant has observed multiple actors cite a May 13 announcement that appeared to be shared with DARKSIDE RaaS affiliates by the operators of the service. This announcement stated that they lost access to their infrastructure, including their blog, payment, and CDN servers, and would be closing their service. Decrypters would also be provided for companies who have not paid, possibly to their affiliates to distribute. The post cited law enforcement pressure and pressure from the United States for this decision. We have not independently validated these claims and there is some speculation by other actors that this could be an exit scam.*

Beginning in November 2020, the Russian-speaking actor "darksupp" has been advertising DARKSIDE RaaS on the Russian-language forums "exploit.in" and "xss.is". And interestingly, in the past few days both of these sites have indicated that they would no longer host ads and forums for Ransomware services, stating that it was drawing too much unwanted attention from law enforcement. Since that's also big news on the ransomware front, I'll have more to say about that a bit later.

But last month, in April 2021, darksupp posted an update for the "Darkside 2.0" RaaS that included several new features and a description of the types of partners and services they were currently seeking. Affiliates retain a percentage of the ransom fee from each victim. Based on forum advertisements, the RaaS operators take 25% for ransom fees less than $500,000, but this decreases to 10 percent for ransom fees greater than $5 million.

In addition to providing builds of DARKSIDE ransomware, the operators of this service also maintain a blog accessible via TOR. The actors use this site to publicize victims in an attempt to pressure these organizations into paying for the non-release of stolen data. A recent update to their underground forum advertisement also indicates that actors may attempt to DDoS victim organizations. The actor darksupp has stated that affiliates are prohibited from targeting hospitals, schools, universities, non-profit organizations, and public sector entities. This may be an effort by the actor(s) to deter law enforcement action, since targeting of these sectors may invite additional scrutiny. Affiliates are also prohibited from targeting organizations in Commonwealth of Independent States (CIS) nations.

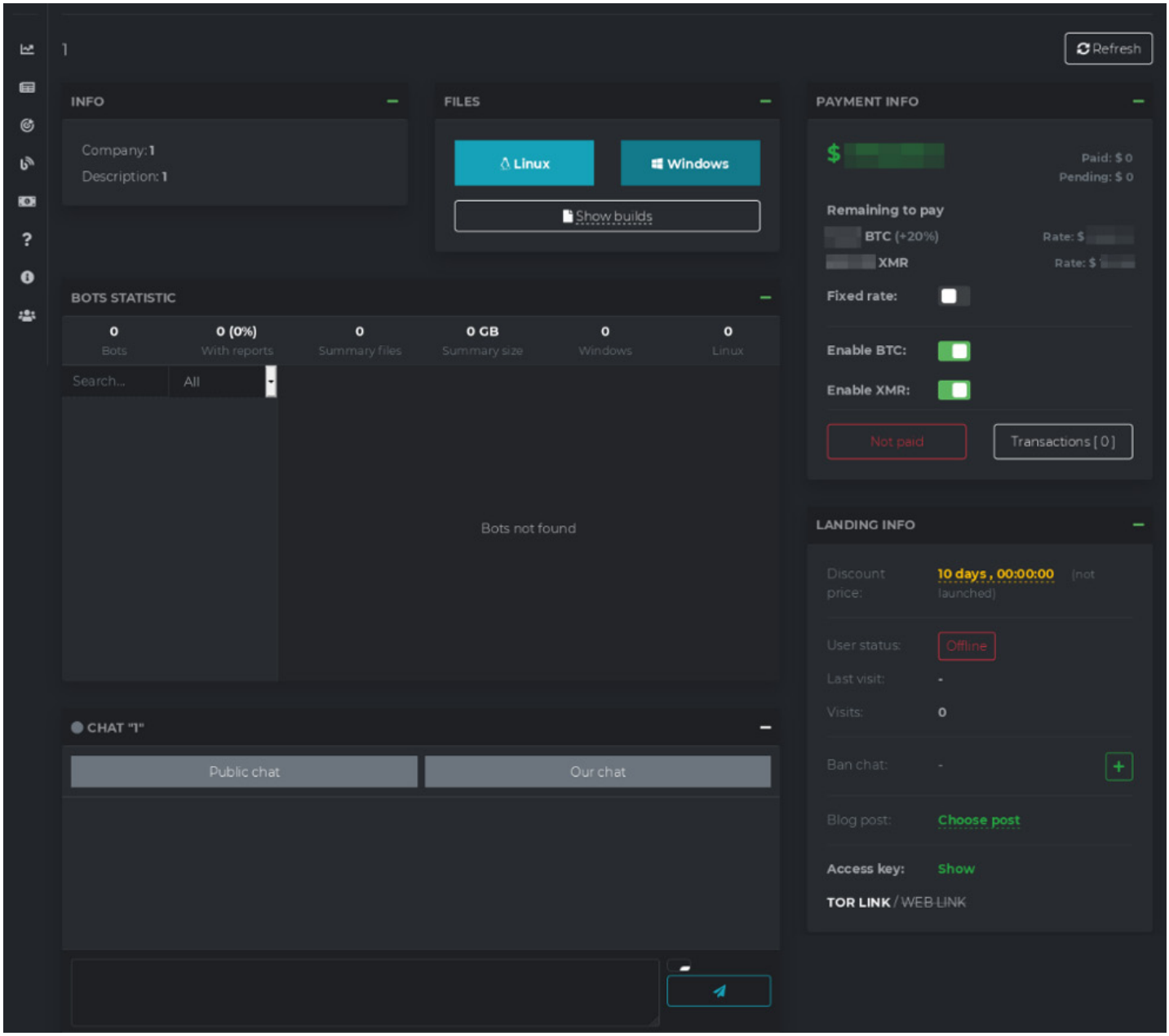
The November 2020 advertisement boasts the features:

- Ability to generate builds for both Windows and Linux environments from within the administration panel.
- Encrypts files using Salsa20 encryption along with an RSA-1024 public key.
- Access to an administrative panel via TOR that can be used by clients to manage Darkside builds, payments, blog posts, and communication with victims.
- The admin panel includes a Blog section that allows clients to publish victim information and announcements to the Darkside website for the purposes of shaming victims and coercing

them to pay ransom demands.

The April 14th update adds:

- Automated test decryption. The process from encryption to withdrawal of money is automated and no longer relies on support.
- Available DDoS of targets (Layer 3, Layer 7)
- Seeking a partner to provide network accesses and a person or team with pentesting skills



DARKSIDE RaaS affiliates are required to first pass an interview, after which they're provided access to an administration panel. Using this panel, affiliates can perform various actions such as creating a ransomware build, providing content for the DARKSIDE blog, managing victims, and contacting support. Mandiant has identified at least five Russian-speaking actors who may currently, or have previously, been DARKSIDE affiliates. Relevant advertisements associated with a portion of these threat actors have been aimed at finding either initial access providers or actors capable of deploying ransomware on accesses already obtained. Some actors claiming to

use DARKSIDE have also allegedly partnered with other RaaS affiliate programs, including BABUK and SODINOKIBI (aka REvil).

It should not be surprising that affiliates might be maintaining relationships with more than one RaaS provider at a time. I suppose that at some point the size of the piece of the action taken of RaaS providers will determine which ransomware is deployed.

In their report, the FireEye / Mandiant guys provide detailed affiliate-specific information about three specific affiliates. I won't go into each of them here. But it was interesting to see that each of the three were distinct and different from the others in their means of initial penetration and movement within networks once they are in. The only obvious link between the three was their obviously well-considered choice of the Darkside ransomware package.

They conclude the general discussion by writing:

> *"We believe that threat actors have become more proficient at conducting multifaceted extortion operations and that this success has directly contributed to the rapid increase in the number of high-impact ransomware incidents over the past few years. Ransomware operators have incorporated additional extortion tactics designed to increase the likelihood that victims will acquiesce to paying the ransom prices. As one example, in late April 2021, the DARKSIDE operators published a press release stating that they were targeting organizations listed on the NASDAQ and other stock markets. They indicated that they would be willing to give stock traders information about upcoming leaks in order to allow them potential profits due to stock price drops after an announced breach. In another notable example, an attacker was able to obtain the victim's cyber insurance policy and leveraged this information during the ransom negotiation process refusing to lower the ransom amount given their knowledge of the policy limits. This reinforces that during the post-exploitation phase of ransomware incidents, threat actors can engage in internal reconnaissance and obtain data to increase their negotiating power. We expect that the extortion tactics that threat actors use to pressure victims will continue to evolve throughout 2021.*
>
> *Based on the evidence that DARKSIDE ransomware is distributed by multiple actors, we anticipate that the TTPs — tactics, techniques and procedures — used throughout incidents associated with this ransomware will continue to vary."*

So, thanks to the colossal focus brought to bear by the Colonial Pipeline attack — which, if nothing else, the DarkSide operators certainly regret in retrospect — we've been able to get a detailed look into the operation of a Ransomware As A Service operation.

It's been widely noted that cryptocurrency has been an enabling factor for ransomware since it potentially solves the problem of the bad guys getting away with the goods. But does it really? Let's next take a look at what we find when we follow the money...

Follow The Money

Elliptic was founded eight years ago to develop and deploy blockchain analytics for tracking financial transactions on the blockchain. Tom Robinson, Elliptic's Co-founder and Chief Scientist recently shared what they learned about Darkside after aiming their blockchain analytics at their transactions...

Based upon their intelligence collection and analysis of blockchain transactions they were able to identify the Bitcoin wallet used by DarkSide to receive ransom payments from its victims. This was the wallet that received the 75 BTC payment made by Colonial Pipeline on May 8th.

By following the blockchain backwards they determined that this wallet has been active since March 4th, 2021 and has received a total 57 payments from 21 different wallets. Some of these payment amounts exactly match ransoms known to have been paid to DarkSide by other victims, such as the 78.29 BTC (worth $4.4 million at the time) that was sent by the chemical distribution company Brenntag a few days earlier, on May 11th.

And the affiliate payment for both the Colonial Pipeline and Brenntag ransom payments were transferred to the same Bitcoin address, which suggests that the same affiliate was behind the original infections and intrusions into both of these organizations.

This also revealed that a previously unknown ransom payment for approximately ~$320,000 was made to DarkSide the day before, on May 10th. And those bitcoins originated from the same exchange that was used by Colonial Pipeline. That was presumably just a coincidence since Colonial's payment had already been received in full.

In total, that DarkSide wallet has received Bitcoin transactions since its March inception totaling $17.5 million. We know that DarkSide has been active since last August. So previous ransoms would have been paid to other wallets.

We know what's coming in. And we've seen some affiliate payments going out. What else is going out? Thanks to modern blockchain analytics, the destination wallet of any monies sent from another wallet can be determined.

We know that there were reports that DarkSide had ceased operations and that it had its funds seized. First of all, that's easier said than done and those in the know are highly skeptical that those behind DarkSide would be maintaining a so-called "hot wallet" online. The blockchain is able to accrue transactions to a wallet without it being present. And if it's not online — and/or if its private key is not compromised — it's not possible to confiscate a wallet's funds.

What we do know thanks to blockchain analytics is that the wallet in question was emptied of the $5 million in Bitcoin it contained on Thursday afternoon. Some have imagined that the funds were seized by the U.S government. But, if so, they didn't get the ransom Bitcoins paid to DarkSide since the majority of those coins had previously been moved out of the wallet the Sunday before on May 9th.

By tracing previous outflows from the wallet, Elliptic was able to gain some insights into how DarkSide and its affiliates were laundering their previous proceeds. They found that 18% of the wallet's Bitcoins were sent to a small group of exchanges. And an additional 4% was sent to Hydra, the world’s largest darknet marketplace, which serves customers in Russia and the Eastern bloc. Hydra offers cash-out services alongside narcotics, hacking tools and fake IDs. These allow Bitcoin to be converted into gift vouchers, prepaid debit cards or cash Rubles. If you’re a Russian cybercriminal and you want to cash-out your crypto, then Hydra is an attractive option.

The owners of any wallet are known and identified **only** by their public and private keys — which are cryptographically strong, long random numbers. And bitcoin transactions are conducted between these random numbers, making them inherently anonymous. And in that sense, the blockchain is reminiscent of the Tor network. Traffic goes into Tor nodes and emerges elsewhere such that the interconnections among the endpoints are not directly knowable. But also similar to the Tor network, the appearance of absolute and perfect anonymity begins to collapse as soon as either one — the Tor network or the Bitcoin blockchain — begins to interact with the outside world. By carefully examining and modeling individual transactions on the blockchain, which functions as an immutable public ledger, we **can** know when a ransom victim pays a known sum to a known Bitcoin wallet. That transaction exists because it is recorded on the blockchain and the subsequent movements of its funds can then be followed. Bitcoin mixing services have arisen specifically to fragment, confuse, scatter and gather bitcoin funds to thwart this sort of transaction tracking.

Toshiba Attacked by DarkSide

Last Friday, the French subsidiary of Toshiba Tec Corp which manufactures barcode scanners, Point-of-Sale (PoS) systems, printers, and other equipment said that it was struck by the Darkside ransomware, which has impacted some regions in Europe. Toshiba Tec shut down networks between Japan, Europe, and its subsidiaries to "prevent the spread of damage" while recovery protocols and data backups were implemented.

Reuters reported that the Toshiba subsidiary said that only a "minimal amount of work data had been lost." Toshiba also said: "We have not yet confirmed that customer-related information was leaked externally" though the company did acknowledge that "it is possible that some information and data may have been leaked by the Darkside group."

When this news surfaced Friday, Darkside's leak site was still inaccessible, but ZDNet successfully accessed a cached version of the site which had been archived by Kela's Darkbeast search engine. (https://ke-la.com/our-solutions/) The archived data shows stolen passport scans alongside project documents and work presentations. So it appears that some exfiltration likely occurred. And Darkside's leak record, posted last Thursday, May 13, indicates that over 740GB of data was stolen from Toshiba.

The timing of this is interesting since OT follows by several days the apparent take down of much of Darkside's operational infrastructure... If, in fact, that did actually occur was wasn't, itself, some misdirection.

Ransomware

Ransomware topics off limits here

The real-world inconvenience caused by the Colonial Pipeline attack has brought unwanted scrutiny — unwanted by those being scrutinized — to the entire supporting ransomware ecosystem — from advertising for new affiliates to the laundering of ill-gotten proceeds. As we know, the new model for Ransomware is RaaS — Ransomware as a Service. And offering any service requires bringing the presence of that service to the attention of new potential customers — or in the case of RaaS, new prospective affiliates.

So, it's extremely significant that the two most popular Russian language hacking forums on the dark web, "xss.is" and "exploit.in", after feeling the pressure of that new and definitely unwanted scrutiny, and have reacted by banning all future discussion of ransomware globally.

Last Thursday the Admin of XSS.IS, which has been serving as the central hub for almost all of the top RaaS providers announced that RaaS on the forum is hereby prohibited. All prior posts relating to ransomware will be deleted and no new posts relating to ransomware will be allowed. The Admin's post states that all "Ransomware affiliate programs", "Ransomware rental", and the "sale of lockers" (as they're called) are prohibited, and any existing topics will be deleted.

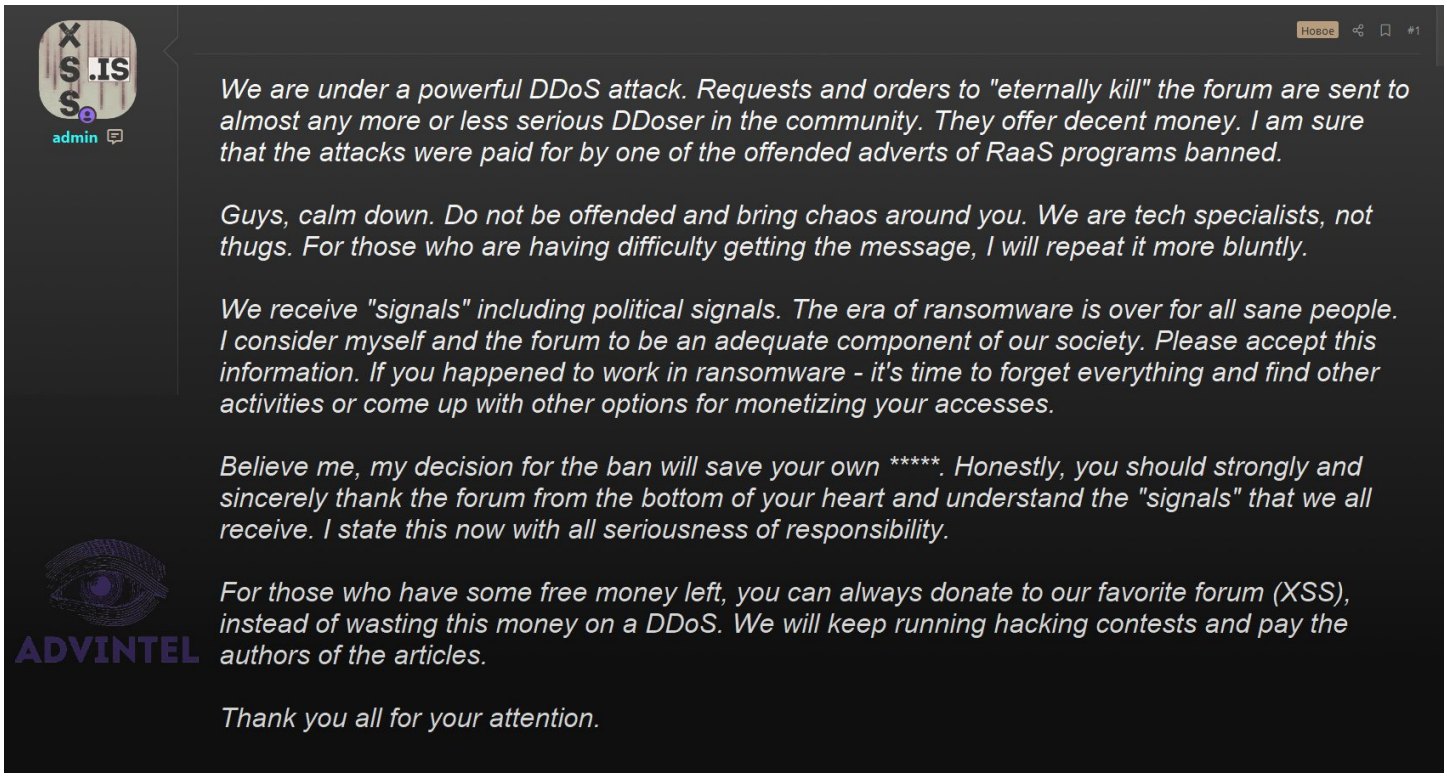
A translation of the Russian language posting is informative. It reads:

> *"**Degradation on the face.** Newbies open up the media, see some crazy virtual millions of dollars that they will never get. They don't want anything, they don't learn anything, they don't code anything, they just don't even think, the whole essence of being comes down to "encrypt - get $". They just run to github, look for locker sorts there and run to encrypt everything they see. Since our forum is aimed at beginners, this factor is important to us.*
>
> ***Too much PR.** Lockers (ransom) have accumulated a critical mass of nonsense, nonsense, hype, noise. When you meet the " Ransomvarny negotiator " Profession , you understand that you are in the looking glass or just crazy. Moreover, 90% of this madness was created artificially, feeding this hype. Those who make good money on this noise (exchanges, insurance, intermediaries, media, etc.)*
>
> ***Ransomware became political.** Peskov is forced to make excuses in front of our overseas "friends" - this is some kind of nonsense and exaggeration. The word ransom was equated with a number of unpleasant phenomena - geopolitics, extortion, government hacking. This word has become dangerous and toxic.*
>
> ***Lockers will exist for a long time.** This phenomenon was too loudly promoted."*

The initial response by several of the ransomware gangs was that they would be leaving XSS.IS and moving to EXPLOIT.IN... that is, until "exploit.in" followed suit the following day, last Friday, and also moved to ban all ransomware discussion and advertising from their forums, too.

And perhaps not surprisingly, on Sunday, the day before yesterday, both forum sites went down due to sustained DDoS attacks, doubtless launched by one or more of the now-banned RaaS gangs.

XSS.IS has been struggling to remain online and here's the posting recently made by its Admin:



Needless to say, this is **very** interesting. The oblique references to "signals" (in double quotes) with "we receive 'signals' including political signals." strongly suggests that there really is an overwhelming amount of anti-ransomware pressure being brought to bear in the wake of the Colonial Pipeline disaster. Of course, it's not up to the Admin of a popular Russian meeting place to unilaterally declare that <quote> "The era of ransomware is over for all sane people." But this does suggest that, moving forward, the organization of Ransomware as a Service will likely be conducted much more quietly and less overtly. And it probably also means that to some extent the exploitation of ransomware "lockers" may return to their origins, being used more by their own developers.

"DarkTracer : DarkWeb Criminal Intelligence" (@darktracer_int / https://darktracer.com/) During my recent digging around, I stumbled upon a live spreadsheet which purports to list the past two years of ransomware attacks by victim, gang and date. At the moment, this list carries the headline: "List of victim organizations (2,203) attacked by Ransomware gangs (34) released on the DarkWeb." The list appears to have been compiled by an organization calling themselves "DarkTracer" (https://darktracer.com/) and it likely lags a bit in its listings since it does not yet list the Colonial Pipeline attack. But to check it out a bit, I noted that it does contain 99 entries for "DarkSide", starting with August 8th of 2020 when it alleges that "Brookfield.com" was attacked. And a bit of Googling revealed that, yes indeed, The Toronto Star carried the report dated August 25th with the headline: "Canadian real-estate company Brookfield Residential suffers data breach by new ransomware group DarkSide".

https://www.thestar.com/business/2020/08/25/canadian-real-estate-company-brookfield-residential-suffers-data-breach-by-new-ransomware-group-darkside.html

Since I would not feel comfortable pointing our listeners at a live spreadsheet being hosted by an apparently benign but still unknown entity, I printed a current snapshot of the spreadsheet to PDF, stripped it of any and all extraneous metadata, and am hosting the PDF at GRC.com. It's a 66-page listing of the past two years (May 1st, 2019 through yesterday, May 17th, 2021) enumerating the who, what and when of those 2,203 Ransomware attacks:

GRC hosted and safe shortcut to the PDF: **https://grc.sc/darktracer**

I included a link to the original live source material with a bold red warning to remind anyone to be careful. It's likely safe, but as we know, spreadsheets have been known to contain vulnerabilities aplenty:

ORIGINAL SOURCE: ***LIVE GOOGLE SHEET*** *(!!! WARNING !!!):*
https://drive.google.com/file/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3/view

Please Leak our Stolen Data!
PeterM / @AltShiftPrtScn 6:17am · 18 May 2021 · Twitter Web App
#Avaddon victim (who didn't pay) asked the attackers to leak their data in full because they were having trouble restoring some files from backup. Threat actor clearly didn't understand, as they responded by saying if the victim didn't cooperate they would leak their data 😂

Security News

Patch Tuesday Review
We're at the 3rd Tuesday of May, so we're able to look back on last Tuesday's comparatively sedate Patch Tuesday. Whereas we have seen past updates delivering fixes for well over 100 flaws, last week was a mere 55 fixes for flaws affecting Windows, Exchange Server, Internet Explorer, Office, Hyper-V, Visual Studio, and Skype for Business. However, that said, there was definitely some excitement...

Of those 55, 4 fixed critical vulnerabilities, 50 were rated Important, and one was Moderate. Three of the vulnerabilities are publicly known, although, unlike last month, none of them are under active exploitation at the time of release... which is good.

But there was one particularly juicy badie that is worrying the industry. It was assigned the CVE of 2021-31166 and it's a potentially wormable remote code execution vulnerability in the HTTP protocol stack of recent releases of IIS for Windows 10. It's wormable because it requires no action on the recipient's part. An unauthenticated remote attacker simply needs to send a specially crafted packet to any vulnerable Windows 10 server to run their own code in the kernel. If that code chose to scan for other publicly accessible (or even internally accessible) hosts, we'd have a new Internet worm on our hands.

Consequently, this ouchy carries a CVSS rating of 9.8 out of 10. And wouldn't you know it?... Some security researcher clown just couldn't help but show off his mad haxor abilities by publishing a working proof of concept which is now up on Github:

https://github.com/0vercl0k/CVE-2021-31166

He wrote: "This is a proof of concept for CVE-2021-31166 ("HTTP Protocol Stack Remote Code Execution Vulnerability"), a use-after-free dereference in http.sys patched by Microsoft in May 2021. According to this tweet the vulnerability has been found by @_mxms and @fzzyhd1."

Even so, this probably won't amount to much because non-corporate users will likely have updated and patched and are nicely isolated behind their NAT routers. And these days few home users are running a public web server. And at the other end of the scale, it's unlikely that any corporate Windows Server installations are nutty enough to be running the latest Windows 10 instances of Server. This bug was recently introduced into the code and only affects Windows 10 Server 2004 and 20H2.

There was also another remote code execution flaw in Hyper-V (CVE-2021-28476), which also scores the highest severity among all flaws patched this month at 9.9 out of 10. Microsoft's advisory said: "This issue allows a guest VM to force the Hyper-V host's kernel to read from an arbitrary, potentially invalid address. The contents of the address read would not be returned to the guest VM. In most circumstances, this would result in a denial of service of the Hyper-V host (bugcheck) due to reading an unmapped address. It is possible to read from a memory mapped device register corresponding to a hardware device attached to the Hyper-V host which may trigger additional, hardware device specific side effects that could compromise the Hyper-V host's security."

In addition, the Patch Tuesday update addresses a scripting engine memory corruption flaw in Internet Explorer (Yes, IE is still around) and 4 more flaws in Microsoft Exchange Server, marking the 3rd month in a row Microsoft has worked to fix the troubled product since the ProxyLogon exploits in March —

- CVE-2021-31207 (CVSS score: 6.6) - Security Feature Bypass Vulnerability (publicly known)
- CVE-2021-31195 (CVSS score: 6.5) - Remote Code Execution Vulnerability
- CVE-2021-31198 (CVSS score: 7.8) - Remote Code Execution Vulnerability
- CVE-2021-31209 (CVSS score: 6.5) - Spoofing Vulnerability

CVE-2021-31207 and CVE-2021-31209 were demonstrated at the 2021 Pwn2Own contest, Orange Tsai from DEVCORE, who disclosed the ProxyLogon Exchange Server vulnerability, is credited with reporting CVE-2021-31195.

Otherwise, the update addresses a large collection of privilege escalation bugs in Windows Container Manager Service, an information disclosure vulnerability in Windows Wireless Networking, and several remote code execution flaws in Microsoft Office, Microsoft SharePoint Server, Skype for Business, and Lync, Visual Studio, and Windows Media Foundation Core.

Miscellany

A review of the first book of "The Frontiers Saga"
https://fab.industries/blog/2021/frontiers-saga/ https://grc.sc/819

On a recommendation from Steve Gibson on his Security Now podcast, I've started reading The Frontiers Saga by self-published author Ryk Brown. This is a review of the first book in the series, called Aurora CV-01. The Frontiers Saga is classical science fiction space opera stuff, best summarised as a cross between Ronald D. Moore's Battlestar Galactica and Star Trek: The Next Generation. Sounds a bit run-of-the-mill at first glance, but it raises eyebrows immediately based on the sheer scope of the work:

> *"The Frontiers Saga is a series of science fiction novels that covers a century of human adventures in space. Part one is 15 episodes, with each episode being released at regular intervals. All story arcs begun within a part are concluded during that part. There will be 5 parts to the series, with 15 episodes per part, for a total of 75 episodes."*

Aurora CV-01, the first book in the franchise, which I've just finished, was originally published ten years ago. Since then, Brown has finished two series, meaning 30 books. That's on average three books (of 200 - 300 pages each) a year. And the guy just keeps on going and going. He's like some sort of anti George R.R. Martin with his output. That alone impressed me enough to give him a shot. And, I must say, I have not regretted it.

60 Minutes / UAP — Unidentified Aerial Phenomena
https://en.wikipedia.org/wiki/Unidentified_Aerial_Phenomena_Task_Force

The Unidentified Aerial Phenomena Task Force (UAPTF) is a program within the United States Office of Naval Intelligence used to "standardize collection and reporting" on sightings of unexplained aerial vehicles. The program was detailed in a June 2020 hearing of the United States Senate Select Committee on Intelligence.

Closing the Loop

The Evolution of a FLoC ID:

- 25 Apr 21, 11:33am / Krv / @Krv
  You asked for someone's FLoC id, here is mine: Your FLoC ID is 5393.

- 16 May 21, 7:01am / Krv / @Krv
  fyi, if you're still interested my floc I'd is now 6501, I'm not sure how often it changes as I haven't been checking it regularly.

Two bits of feedback about last week's "Hail Mary" book recommendation:

- Zap Andersson / @MasterZap
  Yes, @SGgrc Project Hail Mary by @andyweirauthor is indeed AWESOME. Just binged the Audible book (narrator and ... other sounds ... awesome). It's Fudging Great!

- Arnold Ochoa / @a8a
  @SGgrc if you have the chance, you should give @andyweirauthor 's Hail Mary a chance on Audible. No spoilers, but there are things there that just can't be in the book. You'll know what I mean once you read it.

The WiFi Frag Attacks

"The discoverers of the WiFi KRACK attack are back."

The KRACK attack, which we, of course, covered in detail at the time, was a "Key Reinstallation Attack" which was able to break WPA2 encryption by forcing nonce reuse. The same lead researcher and team have been quite busy behind the scenes. They'll be initially presenting their new set of "FragAttacks" at the forthcoming USENIX 2021 conference and then later in much greater detail and depth during this summer's BlackHat 2021 conference.

They discovered three fundamental vulnerabilities inherent in the **design** of the WiFi protocol. In other words, not implementation errors specific to any one or more particular devices, but rather mistakes in the design of WiFi itself. And along the way they also discovered a handful of specific WiFi protocol **implementation** errors.

Here's how they introduced and framed their discoveries:

> We present "FragAttacks" (fragmentation and aggregation attacks) which is a collection of new security vulnerabilities that affect Wi-Fi devices. An adversary who is within range of a victim's Wi-Fi network can abuse these vulnerabilities to steal user information or attack devices. Three of the discovered vulnerabilities are design flaws in the Wi-Fi standard and therefore affect most devices. On top of this, several other vulnerabilities were discovered that are caused by widespread programming mistakes in Wi-Fi products. Experiments indicate that **every** Wi-Fi product is affected by **at least one** vulnerability and that most products are affected by several vulnerabilities.
>
> The discovered vulnerabilities affect all modern security protocols of Wi-Fi, including the latest WPA3 specification. Even the original security protocol of Wi-Fi, called WEP, is affected. This means that several of the **newly** discovered design flaws have been part of Wi-Fi since its release in 1997! Fortunately, the design flaws are difficult to abuse because doing so requires user interaction or is only possible when using uncommon network settings. As a result, in practice the biggest concern are the programming mistakes in Wi-Fi products since several of them are trivial to exploit.
>
> The discovery of these vulnerabilities comes as a surprise, because the security of Wi-Fi has in fact significantly improved over the past years. For instance, previously we discovered the KRACK attacks, the defenses against KRACK were proven secure, and the latest WPA3 security specification has improved. Unfortunately, a feature that could have prevented one of the newly discovered **design** flaws was not adopted in practice, and the other two **design** flaws are present in a feature of Wi-Fi that was previously not widely studied. This shows that it remains important to analyze even the most well-known security protocols. Additionally, it shows that it's essential to regularly test Wi-Fi products for security vulnerabilities, which can for instance be done when certifying them.
>
> To protect users, security updates were prepared during a 9-month-long coordinated disclosure that was supervised by the Wi-Fi Alliance and ICASI. If updates for your device are not yet available, you can mitigate some attacks (but not all) by assuring that websites use HTTPS and by assuring that your devices received all other available updates.

I was not familiar with the abbreviation "ICASI" which they referred to in their opening. So I looked it up. It is either the "International Culinary Arts and Sciences Institute" or the "Industry Consortium for Advancement of Security on the Internet." I'm pretty sure it's the latter.

They then provide a demonstration showing three examples of an adversary abusing a few of these vulnerabilities. The first uses the aggregation design flaw to intercept sensitive plaintext information, in this instance the target's username and password. Then they demonstrate how an adversary can exploit insecure IoT devices by remotely turning on and off a smart power socket. And, finally, they demonstrate how the vulnerabilities can be abused as a stepping stone to launch more advanced attacks. In this case they specifically demonstrate how an adversary can take over a Wi-Fi connected Win7 inside a local network.

So, these various Wi-Fi flaws can be abused in two ways: Given the proper conditions they can be abused to steal sensitive data. And an adversary can also abuse the Wi-Fi flaws to attack devices within a victim's home network.

They felt that the greatest practical risk was likely the ability to abuse the discovered flaws to attack devices in someone's home network. They noted (as I often lament) that many smart home and IoT devices are rarely updated, and that Wi-Fi security is the last line of defense that prevents someone from attacking these devices. But, unfortunately, due to the discovered vulnerabilities, this last line of defense can now be bypassed as shown in their examples of remotely controlling a smart power plug and by taking over a Win7 system.

These Wi-Fi flaws can also be abused to exfiltrate transmitted data. Their opening demonstration shows how this can be abused to obtain the username and password of the victim when they use the NYU website. However, when a website is configured with HSTS to always force the use HTTPS as an extra layer of security, which nowadays close to 20% of websites are, the transmitted data cannot be stolen. And they note that several browsers now warn the user when HTTPS is not being used during the submission of forms. And they also note that although not always perfect, recent mobile apps are, by default, using HTTPS and are therefore also obtaining the protection of TLS.

Plaintext injection vulnerabilities:

Several implementation flaws can be abused to easily inject frames into a protected Wi-Fi network. For example, an adversary can often inject a carefully constructed unencrypted Wi-Fi frame. This can be leveraged into a DNS spoofing attack to trick the client into using a malicious DNS server. And when used against routers this can also be abused to bypass the NAT/firewall to allow the adversary to subsequently attack devices in the local Wi-Fi network.

So how can an adversary construct unencrypted Wi-Fi frames so they are accepted by a vulnerable device? It turns out that some Wi-Fi devices will simply accept any unencrypted frame even when they are connected to a protected Wi-Fi network! So this means that the attacker doesn't have to do anything special! Two of four tested home routers were affected by this vulnerability, several IoT devices were affected, and some smartphones were affected, and many Wi-Fi dongles on Windows will incorrectly accept plaintext frames when they are split into several (plaintext) fragments. The fragment reassembly process simply sidesteps the check for encryption.

They also found that some devices will accept plaintext aggregated frames that look like handshake messages. So an adversary can exploit this by sending an aggregated frame where the start of the frame resembles a handshake message but whose second subframe contains the packet that the adversary wants to inject. This slips the inbound frame past the naïve Wi-Fi parser's state machine. Such vulnerable devices first interpret the frame as a handshake message then pass it on. But during subsequent processing it will be seen as an aggregated frame. So one part of the code will think the frame is a handshake message and will accept it even though it's not encrypted. Then another part of the code will see it as an aggregated frame and will process the packet that the adversary wants to inject.

And, finally, several devices process broadcasted fragments as unfragmented frames and will accept broadcast fragments when sent unencrypted. So an attacker can abuse this to inject packets by encapsulating them in the second fragment of a plaintext broadcast frame. (Did anyone mention that security is difficult?)

Those were clearly implementation mistakes. But as I noted we also have fundamental design flaws:

The first design flaw is in the frame aggregation feature of Wi-Fi. This feature increases the overall speed and throughput of a network by combining multiple small frames into a single larger aggregated frame. To implement this feature, the header of each frame contains a flag to indicate whether the (encrypted) transported data contains a single or an aggregated frame.

But, unfortunately, this “is aggregated” flag is not authenticated and can be modified by an adversary leading to a victim being tricked into processing the encrypted transported data in an unintended manner. This can be abused to inject arbitrary network packets by tricking the victim into connecting to their server and then setting the "is aggregated" flag of carefully selected packets. They said that nearly every device they tested was vulnerable to this attack. And this ability to inject packets can be abused to intercept a victim’s traffic by making it use a malicious DNS server.

This design flaw could be fixed by authenticating the "is aggregated" flag and the Wi-Fi standard does contain a feature to authenticate this flag. but this defense is not backwards-compatible so it cannot be used in practice without breaking the connectivity of all devices that don't use it.

Then we have the “Mixed key attack” design flaw:

This one abuses the deliberate frame fragmentation feature which is also built into Wi-Fi. This feature increases the reliability of a connection by deliberately splitting larger frames into smaller fragments. When doing this, every fragment that belongs to the same frame is encrypted using the same key. However, the receivers of these frames are not required to check the keys of these individually fragmented packets. So, if present, they will dutifully reassemble fragments decrypted using different keys. And this permits an attacker to slip their own packets into the mix. In practice this can allow an adversary to exfiltrate selected client data. Unlike the unfixable “is aggregated flaw” above, this one can be fixed in a backwards-compatible manner simply by only reassembling fragments that were decrypted using the same key — since anything else would be an attack.

The third and final fundamental design flaw is the “fragment cache attack”

This one is quite obscure, but still: When a Wi-Fi client disconnects from the network, the device is not required to flush and remove any non-reassembled fragments from memory. The researchers provide the examples that this could be abused against hotspot-like networks such as “eduroam” and “govroam” and against enterprise networks where users distrust each other. In those cases, selected data sent by the victim can be exfiltrated. This is achieved by injecting a malicious fragment which will remain in memory in the shared access point's fragment cache. When the victim then connects to the access point and sends a fragmented frame, selected fragments will be combined (reassembled) with the injected fragment which was originally provided by the attacker.

Though this one is really obscure, it, too, can be repaired in a backwards-compatible manner simply by causing endpoints to flush any residual fragments from memory whenever the connection state of any connection changes.

And we wrap this up by coming back to a few remaining implementation vulnerabilities:

- Some routers will forward handshake frames to another client even when the sender hasn't authenticated yet. This vulnerability allows an adversary to perform the aggregation attack, and inject arbitrary frames, without user interaction.

- Another extremely common implementation flaw is that receivers do not check whether all fragments belong to the same frame, meaning an adversary can trivially forge frames by mixing the fragments of two different frames.

- Additionally, against several implementations it is possible to mix encrypted and plaintext fragments.

- Finally, some devices don't support fragmentation or aggregation, but are still vulnerable to attacks because they process fragmented frames as full frames. Under the right circumstances this can be abused to inject packets.

The researchers reached out and notified all relevant parties nine months ago so that the problems that could be fixed would be fixed, and so that any devices that were being updated would have the benefits of these fixes. Of course, IoT devices are not currently receiving updates to their Wi-Fi stacks and very few, if any, can ever be updated. Fortunately, the attacks are all edge cases, are difficult to implement in practice, and all require an attacker within radio range of the target. Still, they are just one more reason to always place any questionable devices onto their own network.