Security Now! #735 - 10-08-19

Makes Ya WannaCry

This week on Security Now!

This week we reveal a miracle mistake made by a hacker more than years ago that saved the world from devastating ransomware. But first we catch up on recent ransomware activities, examine the detailed handoff from the GandCrab shutdown and the Sodinokibi startup, a welcome change in Microsoft's Extended Security Update policy for Windows 7, a nasty 0-day RCE in vBulletin, and a bit of nice SQRL news.

HALLOWEEN
What scares you the most?
"Werewolves!"
-Paul
What scares you the most?
"Sharks"
-Nina
What scares you the most?
"The demise of Moore's law and its ramifications for modern computing innovation"
-Dylan
What scares you the most?
"Ghosts!"
-Catherine

The SQRL World Tour

Dublin, Ireland, Gothenburg, Sweden, and concluding with a great panel discussion sponsored by LogMeIn's LastPass in Boston. One more event scheduled...

Security News

We can't get away from Ransomware

The security firm Armor has been tracking ransomware attacks across the US and last week published an updated report on the state of the chaos. In total, more than 500 US schools were hit by ransomware in 2019, and just in the previous two weeks, 15 US school districts -- encompassing 100 schools -- were hit.

Armor tracked ransomware infections at a total of 54 educational organizations -- school districts and colleges -- accounting for disruptions at over 500 schools. And ransomware attacks appear to have picked up further steam in just the last two weeks, with 15 school districts (accounting for over 100 K-12 schools) getting hit in the first weeks of the new school year.

Of these 15 most recent ransomware incidents, Armor said that 5 were caused by the Ryuk ransomware.

Connecticut was hit by ransomware infections at seven school districts so far during 2019, giving them the dubious honor of being the state whose educational institutions were compromised more than any other this year.

And while Connecticut was visited by the greatest number of ransomware infections targeting school districts, it was the state of Louisiana that handled the attacks the best. As we noted at the time in July, Governor John Bel Edwards declared a state of emergency in response to a wave of ransomware infections that hit three school districts. The governor's actions rallied multiple state and private incident response teams together and helped their impacted school districts recover before the start of the new school year... WITHOUT paying the hackers' ransom demand.

The Armor report doesn't specify which districts paid the ransom demand and which did not since not all this information is currently available. However, based on currently available information we know that Crowder College of Neosho, Missouri, reported receiving the highest ransom demand of all school districts, with hackers requesting a whopping $1.6 million to provide the district with the means to decrypt its systems.

And there is also some uncertainty since the level of reporting is inconsistent. The antivirus company Emsisoft reported that it had identified 62 ransomware incidents impacting US schools in 2019, that these 62 incidents took place at school districts and other educational establishments, and that they impacted the operations of 1,051 individual schools, colleges, and universities, more than double the number reported by Armor, at 500.

But regardless of the differing number of impacted schools identified and reported by Armor and Emsisoft, both show a sudden spike in the targeting of US educational institutions with ransomware. And we have previously noted the various reasons why educational districts and municipalities have been identified by attackers as ripe targets of opportunity.

We can obtain some sense for how this 2019 year compares with last year, since, according to a report from the K-12 Cybersecurity Resource Center, in 2018, only 11 of 119 cyber-incidents were attributed to ransomware, thus many fewer than the 54 and 62 ransomware incidents reported so far in 2019 by Armor and Emsisoft, respectively.

The only government sector targeted by ransomware MORE than schools and colleges were local municipalities, which saw 68 ransomware incidents during the first nine months of 2019.

And… In response to this summer's flurry of high profile successful and expensive attacks, last week the US Senate passed a bill named the “DHS Cyber Hunt and Incident Response Teams Act”, which aims to create incident response teams for helping private and public entities to defend against cyber-attacks, including ransomware. The bill had already passed through the House, so it's expected to be signed into law by the president in the coming months.

Meanwhile, in the private sector...

We also previously covered the ransomware incident at the large aluminum producer Norsk Hydro. The remediation cost was originally estimated at $40 million, but it is now expected to hit $70 million. But even more expensive is the recent report that Demant, one of the world's largest manufacturers of hearing aids, expects to incur losses of up to $95 million following a ransomware infection that hit the company last week.

Demant's troubles began at the start of the month, on September 3, when in a short statement on its website, the company said it was shutting down its entire internal IT infrastructure following what it initially described as "a critical incident." What happened to the company's network we'll never know, as Demant never revealed anything except that its "IT infrastructure was hit by cyber-crime." Reports in Danish media soon pegged the incident as a ransomware attack, it did bear all of the hallmarks from the outside. From its own statements, the company's entire infrastructure was severely impacted... and nothing can do that quite like a prolific ransomware attack. Demant's enterprise resource planning system, its production and distribution facilities in Poland, its production and service sites in Mexico, cochlear implants production sites in France, amplifier production site in Denmark, and its entire Asia-Pacific network were all taken down.

And companies typically recover after simple data breaches within days; however, Demant has required weeks, it is still recovering assets today, and it expects to take two more weeks to recover in full. This pattern of destruction that takes months to recover from is usually only seen after severe ransomware infections.

And since these systems are all important to its ongoing business, while the company's staff have been recovering its IT infrastructure, the biggest losses came from the impact of not having access to these systems in the first place. The company reported "delays in the supply of products as well as an impact on our ability to receive orders." Consequently, these various business upheavals have been a disaster for the company's bottom line. In a message to its investors, Demant said it expects to lose somewhere between $80 million and $95 million.

That sum would have been even higher, but the company expects to cash in a $14.6 million cyber insurance policy. Most of the losses arose from lost sales, and the company not being able to fulfill orders. The actual cost of recovering and rebuilding its IT infrastructure were only around $7.3 million -- much less than $80 to $95 million.

In a press release last week Demant said: "Approximately half of the estimated lost sales relates to our hearing aid wholesale business. The incident has prevented us from executing our ambitious growth activities in some of the most important months of the year - particularly in the US, which is our biggest market. A little less than half of the estimated lost sales relates to our retail business where a significant number of clinics have been unable to service end-users in a regular fashion. We estimate that our retail business will see the biggest impact in Australia, the US and Canada followed by the UK. The vast majority of our clinics are now fully operational, however, due to the effect of the incident on our ability to generate new appointments during September, we expect some lost sales in the next one or two months, which is also included in the current estimate.

"Our remaining business activities, Hearing Implants, Diagnostics and Personal Communication, have also been impacted by the incident, but with a relatively smaller overall Group impact due to the nature and size of these businesses," it added. Demant indicated that it expects the incident to have a long-lasting effect on its bottom line. Previous customers may have been driven to a competitor during the Demant outage and they might never return.

It’s certainly useful that they were insured, but the insurance payout didn’t even begin to cover the whole cost of restoring all services -- not to mention the lost customers.

A three-hospital system decides to pay up

An Alabama hospital system with three hospitals has chosen to pay its attackers after a ransomware attack knocked its systems offline exactly a week ago, last Tuesday, Oct. 1st. Officials at the DCH Health System declined to say how much the hospitals paid for the decryption key, but noted that they have started a “methodical” process of system restoration.

According to a website notice:

> In collaboration with law enforcement and independent IT security experts, we have begun a methodical process of system restoration. We have been using our own DCH backup files to rebuild certain system components, and we have obtained a decryption key from the attacker to restore access to locked systems.
>
> We have successfully completed a test decryption of multiple servers, and we are now executing a sequential plan to decrypt, test, and bring systems online one-by-one. This will be a deliberate progression that will prioritize primary operating systems and essential functions for emergency care. DCH has thousands of computer devices in its network, so this process will take time.
>
> We cannot provide a specific timetable at this time, but our teams continue to work around the clock to restore normal hospital operations, as we incrementally bring system components back online across our medical centers. This will require a time-intensive process to complete, as we will continue testing and confirming secure operations as we go.

The system consists of the DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center. DCH administrators said that in the wake of the attack, medical staff have shifted operations into manual mode and are using paper copies in place of digital records... and that new patients are being turned away.

The process will take a while, with the hospitals having a sequential plan in place to decrypt, test and bring the network’s thousands of systems online one-by-one, starting with primary operating systems and essential functions for emergency care. Meanwhile, many hospital services remain offline.

DCH officials said: “Although the attack has impacted DCH’s ability to accept new patients, we are still able to provide critical medical services to those who need it. Patients who have non-emergency medical needs are encouraged to seek assistance from other providers while DCH works to restore our systems.” The hospitals said they are working with law enforcement, outside IT security and forensics experts to address the incident. For their reporting on this, Threatpost asked DCH how the attack was initiated but DCH elected not to reply.

BleepingComputer's coverage of this included the additional information that the infecting agent was our new friend Ryuk, that DCH was still not stating how much they paid for the decryptor, but they did confirm that they have successfully decrypted multiple encrypted servers using the key received from the Ryuk attackers in return for the ransom payment.

Meanwhile, in Australia…

On the same day, Tuesday of last week, seven major hospitals and several smaller health services from Australia's Gippsland and south-west Victoria region were forced to either completely shut down some of their systems or go into manual operation mode following a widespread ransomware infection of their IT systems.

The advisory issued from Victoria's Department of Premier and Cabinet said: “The cyber incident, which was uncovered on Monday, has blocked access to several systems by the infiltration of ransomware, including financial management. Hospitals have isolated and disconnected a number of systems such as Internet to quarantine the infection with the isolation leading to the full shut down of multiple systems, including but not limited to patient records, booking, and management systems.” The advisory added: “Where practical, hospitals are reverting to manual systems to maintain their services.”

As expected in the case of ransomware attacks, though the Victoria Police and the Australian Cyber Security Centre are investigating the incident, they have found no evidence that personal patient information has been accessed... well... if you don't count "encryption" as an "access". :)

And in our final piece of ransomware news for the week…

Bleeping Computer is reporting that our other new friend “Sodinokibi” has successfully assembled an “all star” group of affiliate attackers.

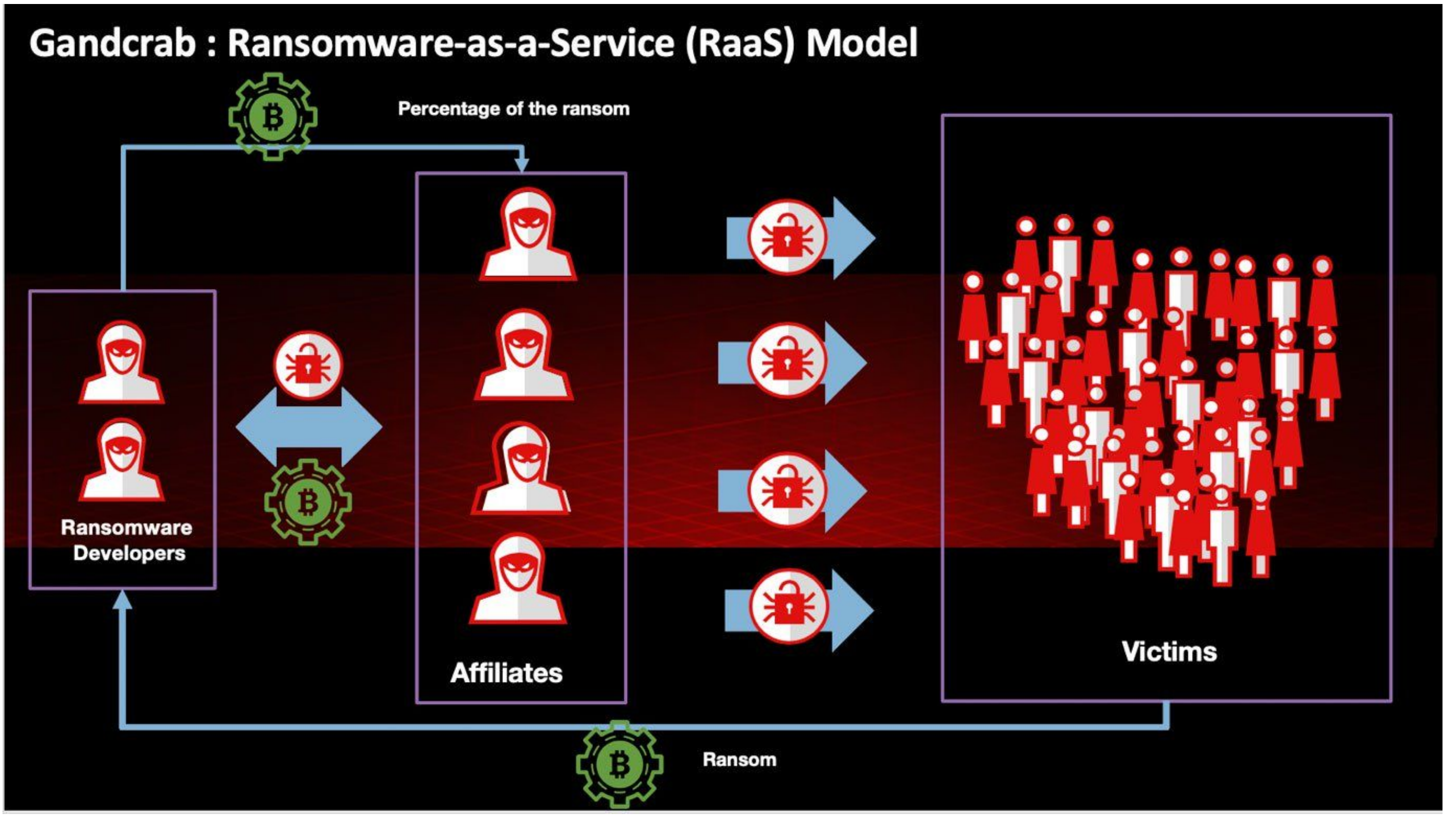
The Sodinokibi Ransomware (REvil) has been making news lately as they target the enterprise, managed service providers (MSPs), and government entities through their hand-picked team of all-star affiliates. These affiliates appear to have had a prior history with the GandCrab RaaS (Ransomware As A Service) model and use similar distribution methods.

Since being discovered in late April exploiting vulnerable WebLogic servers, Sodinokibi has seen wide success through worldwide distribution in exploit kits, phishing campaigns, remote desktop attacks, and large scale attacks through hacked MSP.

In two new reports from McAfee, the Sodinokibi Ransomware has been analyzed to provide information about code similarities between this ransomware and its sort-of predecessor, GandCrab. The affiliates of both RaaS operations have also been analyzed to reveal similarities seen between the two and how many affiliates switched to Sodinokibi as GandCrab began shutting down.

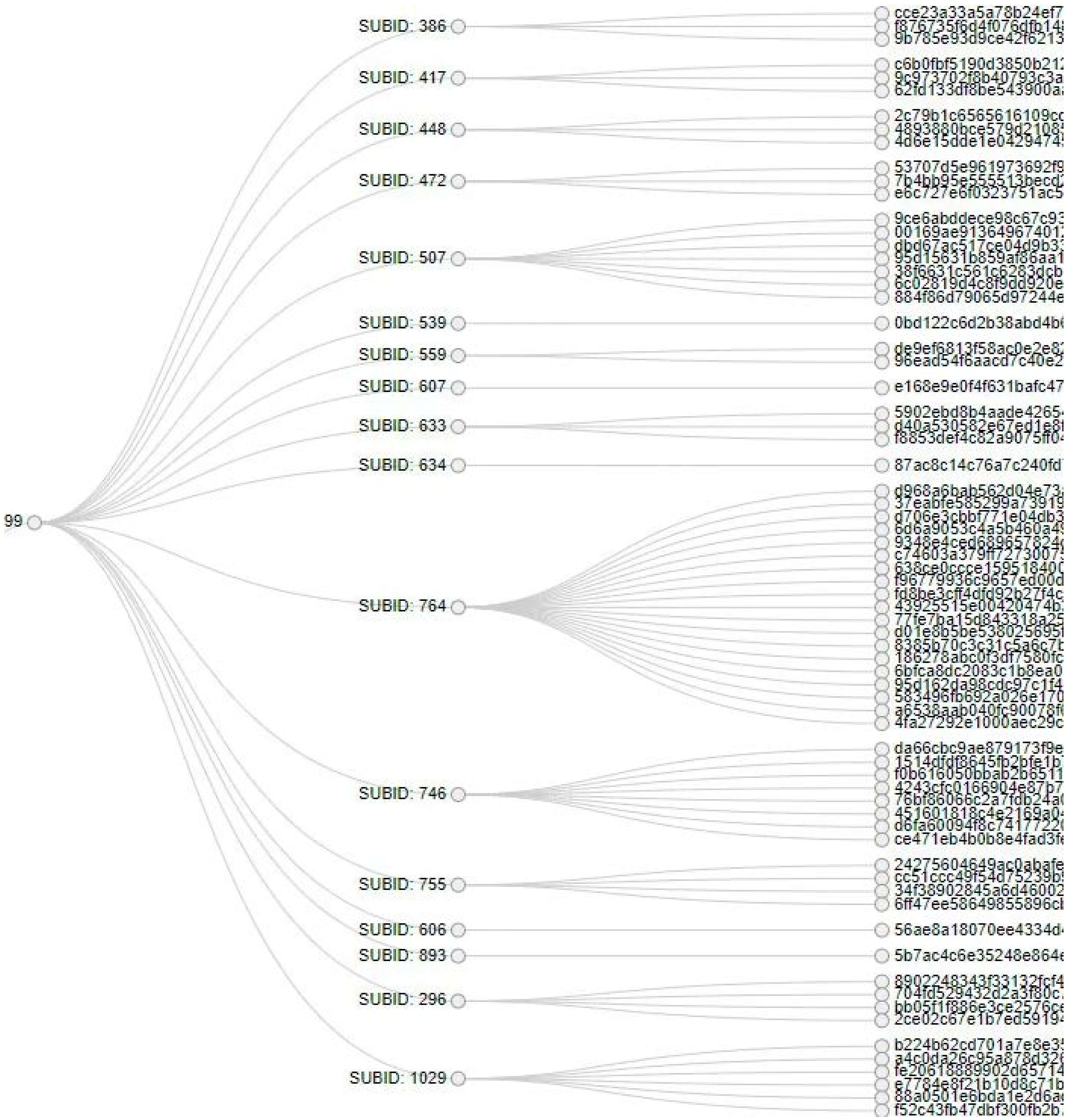
To fully understand Sodinokibi, we should first understand the previous GandCrab operation. One thing that was well known about the GandCrab Ransomware-as-a-Service is that they put together a team of some very qualified and aggressive affiliates. These affiliates showed a wide range of experience in the distribution of malware and advanced technical knowledge regarding managed service provider (MSP) software that allowed them to achieve high volumes of victim compromise even when attacking only a single organization.

And as we've seen, affiliates are well compensated for their "work" (in quotes), earning the lion's share of the ransom payment, with the developer taking a smaller piece of the action, generally only 30 to 40%. That percentage covers their ransomware management and payment system. And through merit-based competition, those affiliates who outperformed the others earn larger pieces of the total.



In the first of these two news research reports, McAfee deeply examined what was known and knowable about the way the GandCrab RaaS operated though some of its higher profile affiliates.

With the GandCrab RaaS, each affiliate was assigned an ID (ID 99 is shown below) that was embedded in the ransomware executables that they distributed. It was also possible for affiliates to generate SubIDs that they could tag an executable with. We do not know what these SubIDs were used for, but could have been for a major affiliate to assign distribution work to one of their partners or simply to track the success of their own different distribution campaigns. In any event, by analyzing hundreds of samples of GandCrab, the McAfee researchers determined that there were approximately 292 affiliates registered with the original GandCrab ransomware, though many were not highly active.



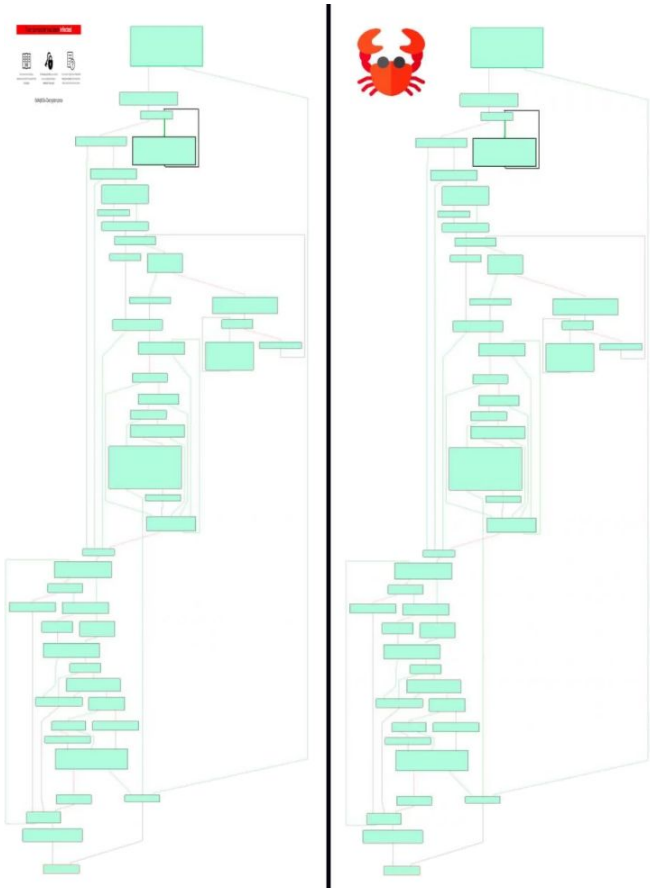
The diagram above shows the spread of ransomware produced by affiliate “99”. This was clearly a “going concern.” McAfee does not currently know which IDs are associated with which particular style of attack, but they’ve said they’re working to assemble those associations.

So now... onto Sodinokibi...

A month before Sodinokibi became active, McAfee noted that the highest profile affiliates suddenly went missing from GandCrab's final 5.2 build. And then, shortly afterward, as we know and discussed at the time, a completely new and unnamed RaaS started being marketed on online hacker forums such as EXPLOIT.IN, where a member named UNKN was recruiting affiliates. This a selective recruitment process only accepted a limited number of highly vetted applicants.

One of the people who replied to the topic in the forum, and vouched for the RaaS, was a member named Lalartu, who stated they were previously a GandCrab affiliate. And then very soon afterward Sodinokibi exploded with ransomware distribution that was very similar to the high profile attacks seen with GandCrab. The evidence collected by McAfee strongly suggests that the GandCrab operators privately informed their top affiliates that they would soon be shutting down and either transferred them to Sodinokibi, or that the affiliates decided to move to the new RaaS. And why wouldn’t they?

When analyzing Sodinokibi samples, McAfee found that Sodinokibi used affiliate IDs and SubIDs in exactly the same way as GandCrab. But the cincher came when the infection code of the two was broken down and placed side by side:



It became quickly clear that the two code bases were, in many places, virtually identical.

When Sodinokibi (REvil) connects back to the ransomware's command and control server, it does so through a randomized runtime-generated URL. And as previously found by other researchers, McAfee confirmed that the URLs generated between the two ransomware families are nearly identical.

So... is Sodinokibi really the new GandCrab?

Despite the preponderance of evidence that suggests it is, it's not possible to be 100% certain. A great deal of malicious code is routinely reused, begged, borrowed or stolen among the criminal underground.

On the "yes, this is the same group" side, we have the strong code similarities and the affiliates who were previously part of GandCrab and are using the same distribution tactics with Sodinokibi. But on the "maybe not" side is that observation that the Sodinokibi operator's approach seems to be significantly different now as opposed to previously. With GandCrab, the operators were open and public with their communications, joked with and poked the research community, and generally had a good time running their operation. But the Sodinokibi operators, have been much more quiet, secretive, and almost reclusive in how the RaaS functions.

BleepingComputer concluded: "While personalities can change, the stark contrast between the two makes BleepingComputer believe that Sodinokibi is being operated by the programmers of GandCrab, while the original operators have since retired or moved on to new things. This would explain the code similarities, yet the different and more secretive nature of the Sodinokibi/REvil RaaS."

... What a world!, eh?

Win7 Extended Security Updates (ESUs) are extended

In happier news, Microsoft has announced that they will accept more money from more people in return for offering to make their Windows 7 extended security updates (which they have to produce anyway) also available to small and medium size businesses, thus broadening its availability beyond its previous exclusive access only to their enterprise volume licensing customers.

I'm using Windows 10 on many machines. It was the OS on the laptop I traveled with to Ireland and Sweden. So all of my loud protestations notwithstanding, I've made a tentative peace with Windows 10. But I do have access to the Long Term Servicing Channel (LTSC) edition, which blessedly allows me to avoid ever having to see Candy Crush Soda Saga and similar Windows 10 consumer atrocities ever appear on the start menu.

But as we recently covered on this podcast, the only reason why Windows 7 and 10 finally swapped their #1 and #2 places at the beginning of this year was the combination of end user capitulation and new system purchases. For the most part, enterprises -- small, medium and large have not budged. And really, why would they? They've got an installed fleet of perfectly working Windows 7 machines causing no one any trouble at all. Everything is fine. Work is getting done.

But in every quarterly and annual report since mid-2015, Microsoft has reminded its shareholders and customers that its business plan for Windows 10 includes "new post-license monetization opportunities beyond initial license revenues." Hmmmmm... Windows as a service.

And forgive me, but I have to rant a bit about this because, yes indeed, what comes along for the ride in Windows 10? Candy Crush Soda Saga, Bubble Witch 3 Saga (I'll never know what happened to Bubble Witches 1 and 2, and I don't care), plus we have March of Empires and Disney's Magic Kingdoms. Not to mention Bing Weather, the Microsoft Solitaire Collection, the Mixed Reality Portal (as if this reality wasn't already mixed enough), Microsoft People (whoever they are), Skype, the Store Purchase App (because, oh yes, please sell me some more of this crap), the Microsoft Wallet to make that even easier, Microsoft Maps (because I definitely want to get the hell out of here!), and a bunch of Xbox and Zune crap (yes!... ZUNE!... let's keep that success alive).

Gee… I cannot imagine why every enterprise, small, medium or large isn't just jumping at the opportunity to put all of those precious gems in front of every employee.

Now, Microsoft is saying that they will ALLOW -ALL- of those businesses, which long ago already purchased and paid for their Windows 7 licenses to continue using them, rather than submit to what Microsoft has deliberately created in Windows 10, if those businesses will effectively repurchase Windows 7 licenses every year moving forward. And remember that what we're really purchasing is the privilege of continuing to receive monthly patches for all of the myriad bugs and mistakes which Microsoft already made in the past and continues to make with every update to their software. If this isn't the definition of a racket, I've never seen one.

I do imagine that this will be a nice new revenue source for Microsoft. If given a choice, businesses WON'T move to Windows 10. Ever. They certainly are not now. Eventually, hardware will die and those replacement PC's will come with Windows 10 decked out with all of its myriad "post license revenue" sources preinstalled.

</rant>

I truly am sympathetic to Microsoft's need to stop servicing their older operating systems. I am. But the only option is to move to a replacement OS that no one wants. And that's not okay.

Jared Spataro, Corporate Vice President for Microsoft 365 said: "Today we are announcing that, through January 2023, we will extend the availability of paid Windows 7 Extended Security Updates (ESU) to businesses of all sizes. Starting on December 1, 2019, businesses of any size can purchase ESU through the cloud solution provider (CSP) program. This means that customers can work with their partners to get the security they need while they make their way to Windows 10."

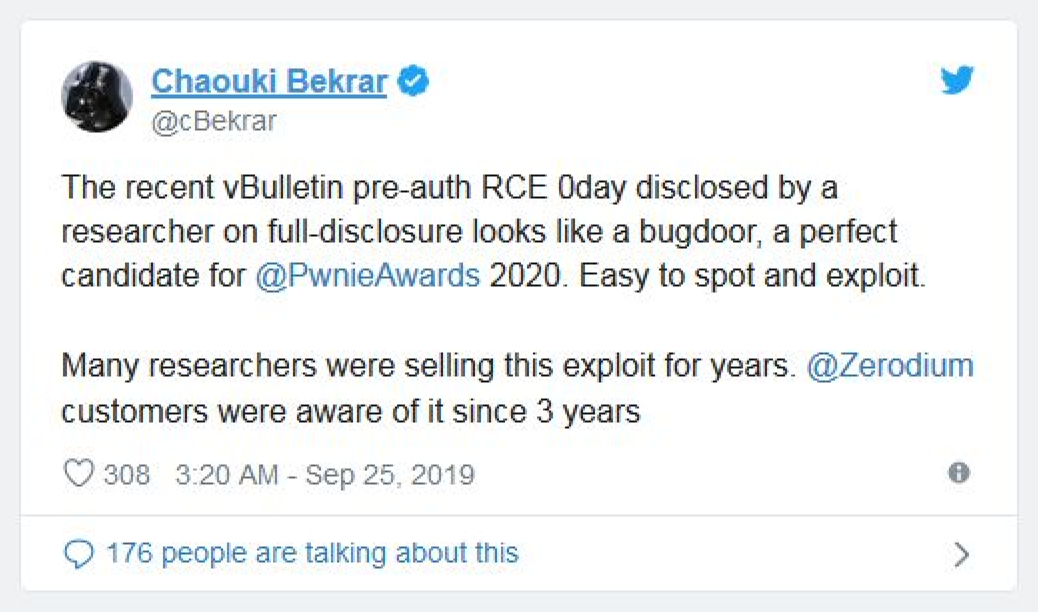
A new Nasty 0-Day RCE in vBulletin

Two weeks ago, back on Monday September 23rd, a 0-day exploit written in 18 lines of Python, which gives a remote attacker unrestricted shell access to any system running the highly popular vBulletin forum software, was anonymously published to the Full Disclosure list, after which attackers wasted no time jumping on and using it to install bots, cryptocurrency miners, and whatever they wished.   https://seclists.org/fulldisclosure/2019/Sep/31

“Tenable Research has analyzed and confirmed that this exploit works on default configurations of vBulletin. Based on the public PoC, an unauthenticated attacker can send a specially crafted HTTP POST request to a vulnerable vBulletin host and execute commands. These commands would be executed with the permissions of the user account that the vBulletin service is utilizing. Depending on the service user’s permissions, this could allow complete control of a host.”

Defcon's site uses vBulletin and Defcon's founder Jeff Moss, told Ars his team took their site down immediately to avoid getting hacked. He said: "We tested it right away and none of our defenses would have saved us. We checked logs and saw no attempts to attack us, but after we patched and went back online, there were two attempts in the first 30 minutes. Definitely active attackers."

But here's something that's a bit sad. We've talked about the questionable ethics of the “We'll buy your bugs at premium prices” company Zerodium. In what struck me as a somewhat tacky and tasteless tweet, Zerodium's CEO and founder, Chaouki (cha ookie) Bekrar, stated that the vulnerability has been privately circulating for years:



Chaouki Bekrar
@cBekrar

The recent vBulletin pre-auth RCE 0day disclosed by a researcher on full-disclosure looks like a bugdoor, a perfect candidate for @PwnieAwards 2020. Easy to spot and exploit.

Many researchers were selling this exploit for years. @Zerodium customers were aware of it since 3 years

♡ 308   3:20 AM - Sep 25, 2019

176 people are talking about this

In other words, for the past three years, any Zerodium customer who wished to could quietly execute any command they wished on the server of anyone running vBulletin… while, in the meantime, knowingly leaving every vBulletin system in the world open and exposed. I suppose that’s the on-the-ground reality of any service such as Zerodium... but it does somehow feel wrong.

SQRL

The SQRL project’s Daniel Persson (who launched SQRL’s Android client, the official WordPress authentication plugin, and a PAM (pluggable authentication module) for Linux/UNIX, shared the following Tweet with the GRC newsgroups:

“Ha.. Added SQRL to my WordPress today.. @kalaspuffar’s plugin enabled this in under 5 minutes.. In and reconnect my admin account and remove email address.. Totally strange that this isn't standard for login everywhere.. :)"

This made my day :)
--
Best regards
Daniel Persson

https://github.com/kalaspuffar/secure-quick-reliable-login

Makes Ya WannaCry

More than two years after the event which briefly rocked the world, and which Marcus Hutchins inadvertently but fortuitously stalled, Sophos recently took a look at the state of the WannaCry worm today. We'd like to say that it's gone but not forgotten... but we can't, because it's far from gone!

So what happened? On May 12th, 2017, organizations across the world were attacked by a new, fast-spreading piece of malware we now know as WannaCry. It is now considered one of the most widespread, and notoriously destructive malware attacks in history, halted only when, out of research curiosity, Marcus Hutchins registered a domain name he had found embedded in the malware which unexpectedly and happily acted as a kill switch. But the kill switch didn't completely kill it, and today, more than two years hence, WannaCry continues to adversely affect thousands of computers worldwide.

In fact, WannyCry has joined the legions of worms including CodeRed, Nimda and MS/Blast that contribute to the constant Internet packet noise for which I long ago coined the term "Internet Background Radiation" ... which is really what it amounts to.

So on that fateful day in May 2017, WannaCry stormed the world. It was made extremely prolific by its use of the EternalBlue vulnerability and exploit which was believed to have been stolen from the US National Security Agency, our NSA, by a group of hackers calling themselves the Shadow Brokers.

And WannaCry provided another vivid example of "the patch gap" which continues to exist today, since the Windows flaw exploited by EternalBlue had already been found, fixed and patched in March 2017's Patch Tuesday, a full two months before WannaCry's trans-Internet rampage. If everyone had patched within those following two months, WannaCry would have knocked but not gotten in. But as it was, a great many Windows systems were behind on their patching so WannaCry entered into a target rich environment and infected something like 200,000 victim machines in the blink of an eye.

Not everyone has patched even now, more than two years later, and WannaCry is not only still alive (and ignoring the kill switch that was designed to stop it), but possibly more alive than ever.

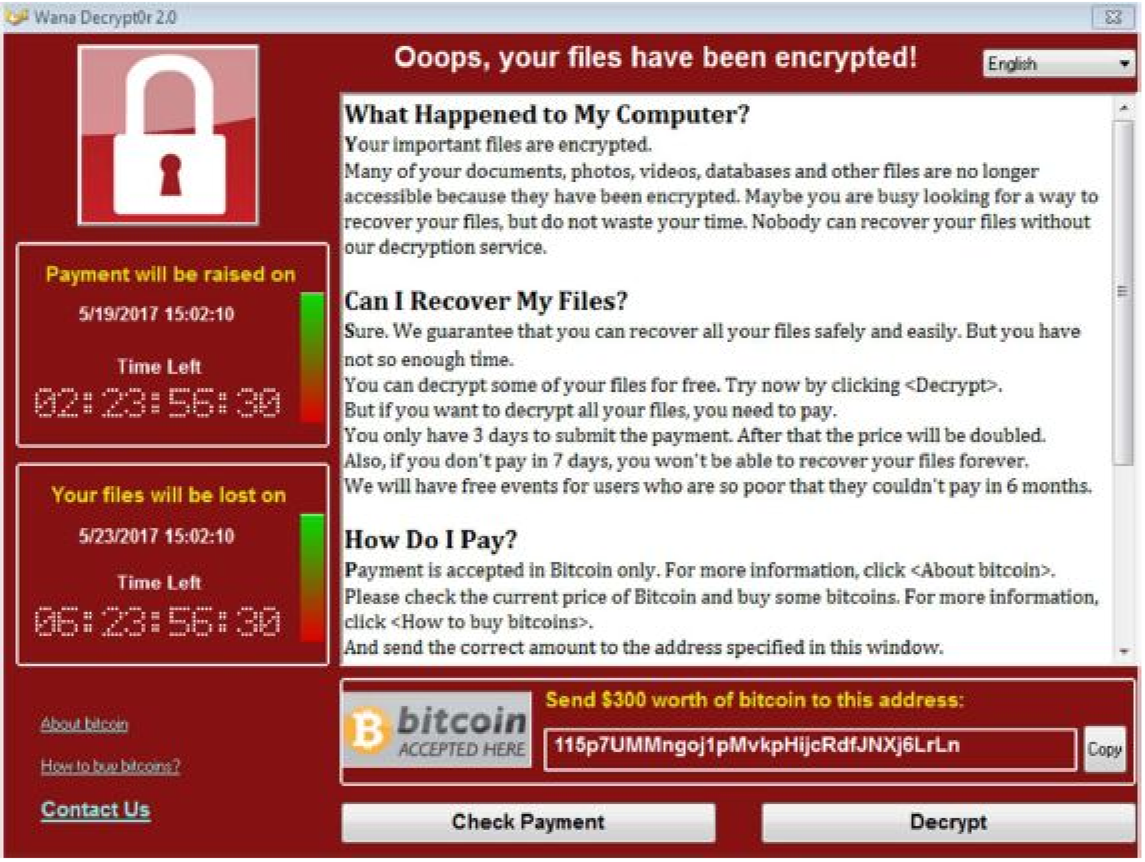
So what's with the original kill switch?

Unless the creators of WannaCry explain their motivation, we'll never know for sure. But two prominent hypotheses exist: Either the attackers wanted to have a way to stop the attack at their discretion, or the more likely is, it was an anti-sandbox evasion technique. Some sandbox environments fake responses from connections to URLs to make the malware think that it is able to access the Internet when, in fact, it's being deliberately prevented from doing so. Since the domain name was deliberately unregistered, the attackers knew that if a DNS lookup succeeded it could have only been because the malware was under analysis in a sandbox, so they could end the attack to hide the true nature of the file.

If this was the motivation for the kill switch, this meant that Marcus' actions effectively turned the entire world into a "sandbox" and shutdown the worm's spread globally.

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

As we know, if this was not done, WannaCry's payload would execute and encrypt the files of the victim, and then post the infamous extortion screen:



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

Payment will be raised on
5/19/2017 15:02:10
Time Left
02:23:56:30

Your files will be lost on
5/23/2017 15:02:10
Time Left
06:23:56:30

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Back then the ransom was a payment of $300 in Bitcoin to recover the files.

There are a couple of interesting notes about how WannaCry was portrayed at the time of its initial outbreak. For example, despite the suggestions that that unpatched Windows XP computers were primarily responsible for WannaCry's rapid spread -- this mistake was due to the fact that some high-profile attacks were XP-based -- more than 97% of WannaCry detections at that time were coming from the newer Windows 7 operating system.

It's also worth noting that, while a computer patched against the EternalBlue exploit is no longer vulnerable to being infected by a remote connection from another WannaCry-infected computer, if that computer was infected before it was patched, it will still try to infect other computers; The anti-EternalBlue patch only prevents the vulnerability from being exploited, not from exploiting others.

And… if nobody had since updated WannaCry, the file that started spreading on May 12th, 2017, would be the same as the file seen in the wild today. But, it turns out, the reality is very different, and much more intriguing…

The New WannaCry:

Sophos' research is based on a signature named CXmal/Wanna-A, the detection name that identifies when a computer, suddenly finds the WannaCry payload (the mssecsvc.exe file) plopped into the C:\Windows directory. On a Sophos-protected machine, the client application immediately blocks and removes this file.

Using this detection data, Sophos has been able to see how many computers are being attacked, repeatedly, by other computers, as well as the file dropped during the attack. These infected machines could be on the same network as the ones being attacked, or possibly anywhere in the world. All we really know about the infected machines that attempt to spread the infection is that they don't have a working antivirus product on them. Otherwise they would have stopped WannaCry and wouldn't be attempting to infect other machines.

In the three month period between October 1, 2018, and December 31, 2018, Sophos logged 5,140,172 detections (not individual computers) of CXmal-Wanna-A. Nearly two years on from the original attack, as nearly every machine that can install the EternalBlue patch has already done so, why are there still so many detections?

As a sanity check, since that data was nearly a year old, Sophos reran their queries looking at just one month of attack data, from August, 2019. They discovered that in that month alone, they had recorded more than 4.3 million attacks against customer machines. That seems like a significant increase, but those numbers can be misleading because the data is based on customer machine feedback, and the number of customer reports changes over time as the size of the customer base changes. That can make it seem like the problem is getting worse.

What was important to note is that the proportion of the total number of attacks targeting Sophos customers in specific countries remained consistent in the data from 2018 and 2019, with machines in the US topping the list of countries most subjected to failed attempts at WannaCry infections.

The fact that WannaCry is still going at all raises some interesting questions:

1. Are all of these machines really still not patched?
2. Why is the kill switch not preventing the infected computers from trying to attack others?
3. Why is no one complaining about files being encrypted?

They knew the answer to question 1 already, as the CXmal/Wanna-A detection is only possible on unpatched machines. To be sure they investigated a random selection of computers to manually verify that they had, indeed, not been patched against EternalBlue, or anything else, in the last two years.   <sigh>

To answer question 2 "Why is the kill switch not preventing the infected computers from trying to attack others?" they know the computers reporting the detections have internet access because that's how they obtain their data. Since those machines are most likely being attacked by infected computers on the same network, it seems likely that those machines would also have internet access. So why isn't the kill switch stopping them?

Analysing the 5.1 million CXmal/Wanna-A detections over the three-month period from October 1 through December 31, 2018, they discovered something unexpected: The malicious file being dropped on these computers was **NOT** the original WannaCry mssecsvc.exe file (MD5: db349b97c37d22f5ea1d1841e3c89eb4). In fact, among the 5.1 million detections, they identified 12,481 unique files.

The original, true WannaCry file was seen only 40 times, a number so low that it could easily be attributed to testing, rather than a real attack.

- 12,005 of the unique files identified (96.1%) were seen fewer than 100 times each.
- 476 of the unique files (3.8%) accounted for an overwhelming 98.8% of the detections.
- Ten files accounted for 3.4 million (66.7%) of the detections, with the top three accounting for 2.6 million (50.1%).

So they analyzed the top 10 most prevalent files and quickly saw that they had all been altered very early in the code. The alterations in all 10 samples bypass the kill switch entirely. This means that these updated WannaCry variants' ability to spread is no longer restrained by the kill switch.

So they examined all of the files they had and discovered the application of four different techniques which had been used to render the killswitch ineffective:

1. Simply removing or changing the kill switch URL. Roughly half of the samples did this, with most just removing the URL completely. The next most common approach was to change the last two letters from "ea" to "ff". Modifying the killswitch domain resulted in these variants of WannaCry being unable to connect. Instead of exiting, they would simply move to the next command, which was to launch the attack.

2. The second method was to change the code to instruct the malware: regardless of the result of the kill switch test, move to the next command (execute the attack).

3. The third method was to replace the kill switch with "nop" (No Operation) opcodes, which means: do nothing. These replaced the code that would check the result of the kill switch connection attempt. So it doesn't check the result and just continues with the attack.

4. The 4th and final method seen was to use a 2 byte "jmp", to jumps over the code that checks the result of the kill switch connection, also resulting in it just continuing the attack.

What's really interesting is that all four of these techniques were implemented by hex editing the original WannaCry malware executable binary file… NOT by recompiling from the original source code. Since anyone who obtains a copy of the executable binary is able to hex edit it, this suggests that many miscreants around the world were attempting to untether and unleash the original WannaCry ransomware worm upon an unsuspecting world.

We know that the original WannaCry kill switch is still crucially important because, in a recent interview of Jamie Hawkins, who worked with Marcus Hutchins on that fateful domain-registering day, Jamie indicated that “in June 2019 alone, the kill switch prevented about 60 million ransomware detonations,” indicating that there are still (potentially) thousands of computers infected with the original WannaCry, and keeping the kill switch domain online is the only thing stopping a second outbreak.

So… if all of those manually hex edited copies of WannaCry have been unleashed, why hasn’t a second massive wave broken out?

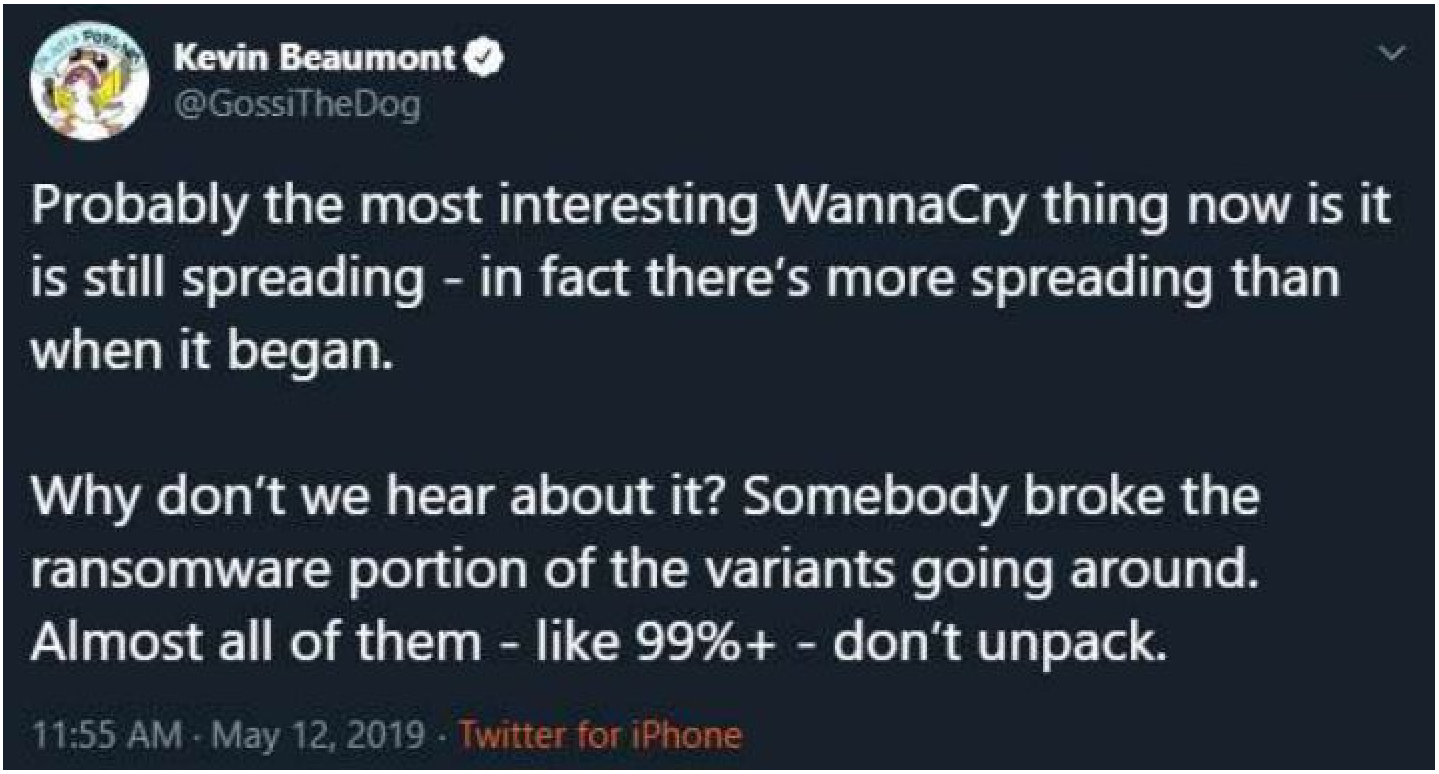
To answer this question, Sophos executed a random selection of samples, including the top ten that were most prevalent on unprotected computers. In each case, no files were encrypted, and no ransom notes were created.

There is one component that spreads the malware to other machines, and then there is a separate component that does the encryption. This second component is contained in a password protected ZIP archive. The contents of the ZIP archive are extracted to the computer and then used to execute the ransomware attack.

In all 2,725 samples, the ZIP archive was corrupt!

Errors appeared after only a few of the archive’s files had been extracted from the contents. That was the discovery they were seeking making everything else make sense. The large volume of detections were due to the lack of a kill switch, but nobody was complaining about encrypted files because almost every sample seen in the wild had a corrupt archive that doesn’t encrypt anything! ***(There but for the grace of God.)***

Sophos researchers were not the only ones to spot this. Back in May, 2019, researcher Kevin Beaumont tweeted the above...



Kevin Beaumont
@GossiTheDog

Probably the most interesting WannaCry thing now is it is still spreading - in fact there’s more spreading than when it began.

Why don’t we hear about it? Somebody broke the ransomware portion of the variants going around. Almost all of them - like 99%+ - don’t unpack.

11:55 AM · May 12, 2019 · Twitter for iPhone

And… it turns out that this broken payload had appeared almost immediately following the original infection.

On May 14, 2017, researchers at Kaspersky discovered a variant of WannaCry that had been uploaded to VirusTotal earlier that day. They shared the sample with researcher Matt Suiche, and in a blog post that same day he confirmed that the sample did **not** have a kill switch, and that the archive was corrupt.

It was also noted that while the sample had been uploaded to VirusTotal, it had not been seen in the wild. This sample led to Sophos' final discovery.

The MD5 hash of the file uploaded to VirusTotal, which doesn't have a kill switch and doesn't encrypt files, is none other than the exact same file they now see causing the highest number of WannaCry detections:

MD5: d724d8cc6420f06e8a48752f0da11c66

It is #1 on the unique file variants list provided earlier, causing 29% of all WannaCry detections in their data. Even more amazing is that the top three files on their list are all variants of this same file. The other two files contain the same corrupt archive; the only difference is in how the kill switch has been removed.

In other words, it's sort of a true miracle that a subtle mistake made just days after the first WannaCry wave prevented the utterly unrestrained and unrestrainable devastation that would have occurred with WannaCry's immediate return.