UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. 20-CV-1217 (LDH)

DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF REQUEST FOR CERTIFICATE OF DEFAULT

I, Gabriel M. Ramsey, declare as follows:

1. I am a partner of the law firm of Crowell & Moring LLP, counsel of record for Plaintiff Microsoft Corp. ("Microsoft"). I make this declaration in support of Microsoft's Request for Certificate of Default. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. DEFENDANTS HAVE NOT RESPONDED TO THIS ACTION OR OTHERWISE REQUESTED THAT THE DOMAINS AT ISSUE IN THIS CASE BE REINSTATED

2. As described more fully below, John Doe Defendants 1-2 ("Defendants") have been properly served the Complaint, summons, and all key orders and pleadings in this action pursuant to the means authorized by the Court in the Temporary Restraining Order and Order for Preliminary Injunction, and these Defendants have failed to plead or otherwise defend the action.

3. As of August 23, 2020, I have not been contacted by any of the Defendants regarding this case or seeking reinstatement of the Necurs botnet control domains.

4. Based upon the Defendants' operation of a sophisticated botnet, and known information regarding the infrastructure at issue, upon information and belief, the Defendants

against whom a notation of default is sought are not infants, in the military or incompetent persons.

II. SERVICE OF PROCESS AND NOTICE UPON DEFENDANTS

A. Defendants Are Likely Aware Of This Proceeding Given The Impact Of The TRO And Preliminary Injunction

5. Defendants are very likely aware of this proceeding simply given the significant impact of the TRO and preliminary injunction on their operations, in combination with the steps Microsoft took to serve process by e-mail and through publication, discussed below.

6. Microsoft executed the TRO on March 10, 2020. Consequently, the Necurs command and control infrastructure was redirected to Microsoft servers. This effectively severed communications between the Necurs-infected devices and the Defendants.

7. By disabling the command and control infrastructure, the operation and growth of the Necurs botnet has been frustrated by the temporary restraining order and preliminary injunction issued by the Court. Because the domains controlling the botnets have been disabled or redirected since March 10, 2020, Defendants have not been able to access their software, which was operating through those domains, and have not been able to communicate with Necurs-infected end-user machines using those domains. This has impeded the Defendants' ability to grow the Necurs botnet and has significantly disrupted their ability to steal online credentials and personal information from the owners of the infected computers. Given the obvious impact on the botnets, Defendants are very likely to be aware of the impact on the botnet and the fact that the instant proceeding is the cause of that impact.

8. Additionally, third-party observers of the Necurs botnet have widely reported about this action, and I have confirmed that the action has been reported in public media. Attached hereto as Exhibits 1-4 are true and correct examples of articles in the public media related to this action.

B. Service By Internet Publication

9. Microsoft has served process by Internet publication, as authorized by the TRO and Preliminary Injunction, which provide that service may be effected by "publishing notice on a publicly available Internet website." Dkt. 11 at p. 12; Dkt. 14 at p. 10. Beginning on March 10, 2020, Microsoft published the Complaint, summons, orders and all pleadings in this action on the publicly available website www.noticeofpleadings.com/necurs. All subsequent pleadings and orders have been made available on that website throughout the case. A link to the website was sent in the service of process e-mail sent to Defendants at the e-mail address determined to be associated with the registered Necurs botnet domain. Attached hereto as Exhibit 5 is a true and correct copy of a screenshot of the publicly available website www.noticeofpleadings.com/necurs.

C. Service By E-mail

10. Microsoft has also served process through e-mail, as authorized by the TRO and Preliminary Injunction, which provide that service may be effected by "transmission by email … to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements." Dkt. 11 at p. 12; Dkt. 14 at p. 10. Through its pre-filing investigation and informal discovery efforts, Microsoft gathered contact information, particularly the e-mail address, associated with the registered Necurs botnet domain. Defendants had provided this e-mail address to the domain registrar when completing the registration process for the domain used in the command and control of Necurs. Microsoft used this contact information to serve Defendants. Subsequently, through discovery responses and identification of historical Necurs domains, Microsoft identified four additional email addresses and served Defendants through those email addresses

11. In this case, the e-mail addresses provided by Defendants to the domain registrars are the most accurate and viable contact information and means of notice and service. Since Defendants provided false names and addresses to the domain registrars, Defendants will have

expected notice regarding their use of the domains by e-mail. Given that Defendants connected to the Necurs infected user computers through these domains, it was crucial for them to remain vigilant as to any change of the domains' status. Since Defendants were able to maintain the Necurs domains active until the execution of this Court's TRO, it follows that Defendants monitored the e-mail accounts to maintain use of the domain registrars' services.

12. Microsoft served by e-mail copies of the Complaint, Court Orders, summons and a link to the pleadings in this action to the email address kaledunning@yahoo.com on March 11, 2020 and to the email addresses thomas_beatty@ymail.com, coastalburns@yahoo.com, jameskampel@yahoo.com and gweo8askuh@mail.ru on March 30, 2020. Despite this robust notice and service, the Defendants have not come forward in this action to defend or seek reinstatement of the Necurs botnet control domains. There has been no response from the Defendants to date in this action.

D. Attempted Notice And Service By Mail

13. Microsoft has investigated each physical mailing addresses associated with the Necurs botnet domains. This information was fabricated by Defendants to conceal their actual physical locations. For example, investigation verified that the mailing addresses used to register domains either do not exist or exist but are associated with fake names, i.e. the defendants do not actually reside at the address. From this, I conclude that the e-mail addresses associated with the domains and described above are the most viable way to communicate with the Defendants in this action. As noted above, Defendants provided these e-mail addresses when registering the domains used in the command and control infrastructure of the botnet making it likely that Defendants monitored messages sent to those addresses.

III. INVESTIGATION REGARDING DEFENDANTS' CONTACT AND IDENTIFYING INFORMATION

14. Microsoft endeavored to identify additional contact information through which Defendants could be served. Over the course of its investigation, pursuant to the Court's

discovery order, Microsoft served subpoenas to attempt to identify further contact information. No further contact information was identified beyond the additional email addresses noted above. Given (a) Defendants' use of aliases and false information, (b) the ease with which anonymous activities can be carried out through the Internet and (c) the sophistication of the Defendants, Microsoft has been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be served by personal service. Notwithstanding these limitations, through the discovery process, the investigation has yielded at least some information, including the ".ru" email address suggesting that Defendants may be located in Russia.

15. I investigated the e-mail addresses to determine whether those pieces of information could be used to identify the real names of Defendants and their physical addresses. I conducted Internet searches to determine whether these pieces of information correlated to real names or physical addresses associated with Defendants. For example, the investigation looked for instances where Defendants may have used these e-mail addresses in contexts other than their anonymous activities that are the subject of this case; for example, in personal exchanges or business affairs on the Internet where they used their real names or addresses. However, despite an extensive effort in this regard, the e-mail addresses did not definitively correlate to any real names or physical addresses. Given Defendants' incentives and practices to conceal themselves, discussed further below, Microsoft believes that it is likely that nicknames, even those resembling real names, are fictitious.

16. During our investigation of e-mail addresses, we encountered only instances in which Defendants had used free e-mail services. To the extent that we were able to serve subpoenas upon such service providers in the United States, we did so, seeking registration and account information for the free e-mail accounts used by Defendants. The subpoena responses revealed that there was no additional identifying information in the records. Defendants were able to sign up using fictitious names. Thus, Defendants were able to conceal their identities and

physical locations. The IP addresses from which Defendants had logged into the free e-mail accounts were associated with anonymization services, which prevented further discovery of Defendants' identities as such IP addresses cannot be definitively associated with Defendants' real identities.

17. For the foregoing reasons, the subpoenas to free e-mail providers did not yield information about the real names or physical addresses of Defendants. Microsoft has used all reasonably available formal and informal means to investigate the true identities of the Defendants. Microsoft has exhausted its ability to investigate Defendants' true identities using civil discovery tools, despite best efforts and the exercise of reasonable diligence to determine Defendants' identities.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 23rd day of August, 2020.

Gabriel M. Ramsey

EXHIBIT 1

BRIAN BARRETT SECURITY 03.10.2020 09:34 AM

How Microsoft Dismantled the Infamous Necurs Botnet

A years-long investigation and global cooperation disrupted one of the biggest botnets ever.

Microsoft has taken the lead on dismantling operations like Necurs before, given the extent to which they threaten Windows devices and their users. PHOTOGRAPH: VINCENT ISORE/GETTY IMAGES

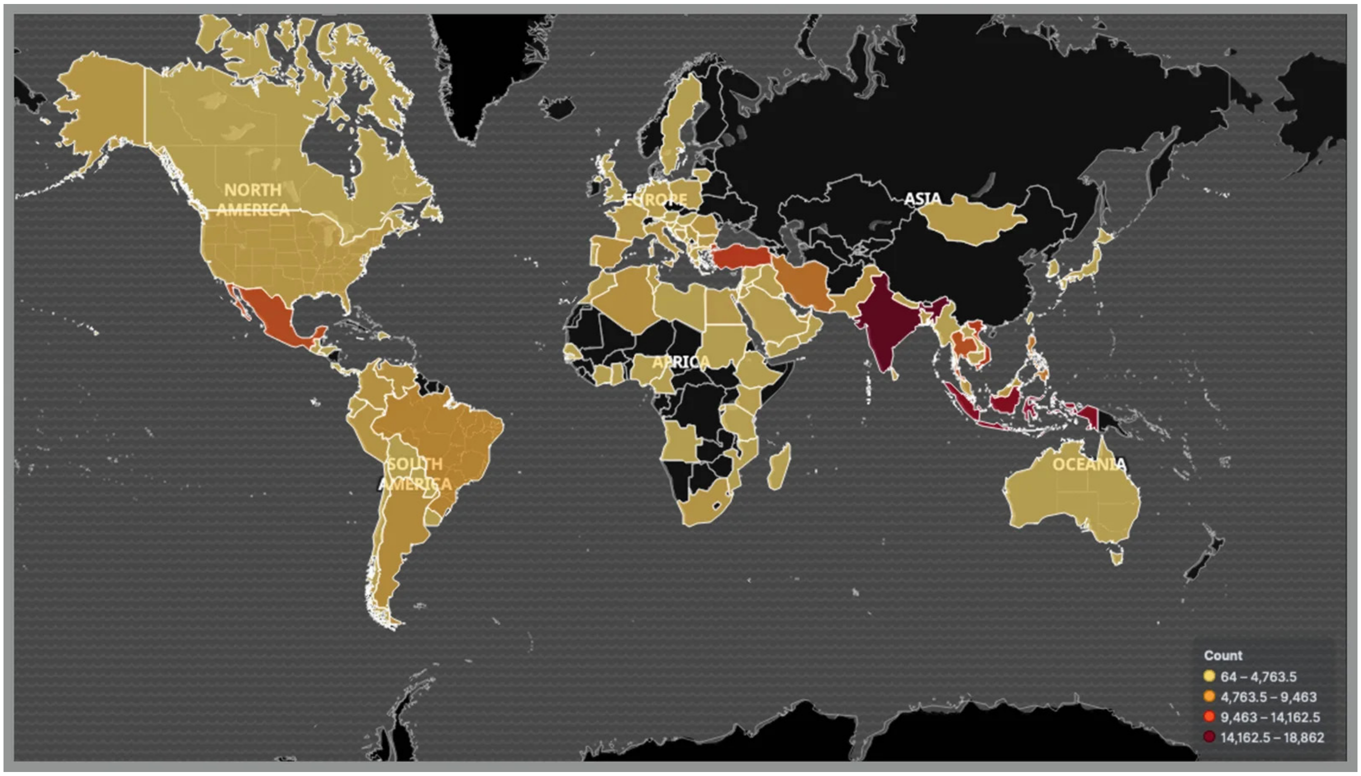
AT THE HEIGHT of its powers, Necurs was one of the most disruptive forces on the internet. A sort of

Swiss Army botnet, over the years it has harnessed more than 9 million computers unwittingly under its control to send spam, distribute ransomware, attack financial institutions, and more. Last week, Microsoft pulled its plug.

Necurs has been silent lately—its most recent significant activity petered out last March—but it still has 2 million infected systems awaiting its next command. By disrupting what remains of the botnet—in coordination with law enforcement and internet service providers across 35 countries, and with the help of cybersecurity firms like BitSight and ShadowServer—Microsoft has effectively prevented Necurs from rising again.

“This disruption is the result of eight years of tracking and planning,” wrote Microsoft corporate vice president Tom Burt in a blog announcing the takedown, “and will help ensure the criminals behind this network are no longer able to use key elements of its infrastructure.” Microsoft declined to comment further, but the company has taken the lead on similar takedowns in the past, given the extent to which operations like Necurs threaten Windows devices and their users.

While botnets are often associated with distributed denial of service attacks, Necurs has a more diverse portfolio. “The reason the Necurs botnet is so pernicious is because the attackers managed to infect so many devices, and leverage this massive botnet for various purposes based on the fact it distributes many other types of malware,” says Yael Daihes, senior security researcher at the content delivery network Akamai. Chief among those is spam; in a criminal complaint filed March 5, Microsoft noted that “one single infected Necurs computer is capable of sending a total of 3.8 million spam emails to over 40.6 million potential victims over a 58 day period.”



A geographic distribution of Necurs infections in the first seven days of March 2020. COURTESY OF BITSIGHT

Necurs is largely a botnet-for-hire, available to distribute whatever malware a client might want. That includes the infamous GameOver Zeus trojan that plagued the internet nearly a decade ago, as well as the Dridex malware deployed by Evil Corp and others. The criminal complaint details the use of Necurs to distribute notorious malware like Locky and Trickbot, as well, like a smuggler for the Legion of Doom. The possibilities are endless, from ransomware to banking-information theft to surveillance.

Necurs can also block antivirus updates in older machines, leading to a host of knock-on problems. “For devices using an outdated Windows 7 without updated antivirus protections, Necurs not only cripples the security mechanism that might result in removal of Necurs from the computing device, it may leave victim’s computing devices exposed to many other types of malware,” the complaint reads.

“Necurs, prior to Microsoft's actions, remained a significant threat, even though it seems to have declined in relevance since 2016,” says Evelyn French, senior analyst at Flashpoint, a security firm that has tracked the botnet.

Necurs was first discovered online eight years ago, and has been linked in the years since to the various malware families that used it for distribution. But the takedown work didn't start in earnest until 2016, when BitSight began a years-long effort to disentangle the botnet, reverse engineering its structure so that Microsoft and others could actually disrupt it. You can’t fight what you can’t see.

It was a hard slog. Necurs isn't a single botnet but a family of at least 11, all presumed to be under the control of the same unidentified Russian criminals. Four of those botnets, BitSight found, were responsible for 95 percent of all infections. Moreover, Necurs uses a particularly sophisticated command-and-control structure to relay information to and from the computers it controls.

In the most basic command-and-control setup, a piece of malware will attempt to communicate with a single domain, from which hackers give instructions. Necurs is far from basic. Rather than rely on a fixed site, it uses a so-called domain generation algorithm, or DGA, to create 2,048 potential domains every four days, giving its zombie computers a lot of flexibility. "It's a function to change the domains it talks to basically every day, every week, every month. That can be variable based on what the person who wrote it wants to be doing," says Dan Dahlberg, BitSight's head of security research. "Today the botnet may try to talk to 50 different domains to try to find the one the actor actually controls. The next day it might change to another 50."

Several botnet families use DGAs. Necurs adds its own twists, though, primarily centered on adaptability. Once an infected machine successfully links up with a Necurs command-and-control domain, it stops reaching out elsewhere until that connection gets broken for whatever reason. Only then does it resort to the DGA. It also uses multiple layers of command-and-control servers, and it enables devices connected to the same server to communicate with others in that cluster and compare notes about what domains are functional.

"It has this kind of defense-in-depth communication structure, almost similar to how a company would structure its internal security tools to have this escape and fallback mechanism," says Dahlberg. "And of course, as these malware families implement more complex methods of communication, it makes disruption and takedowns much more complicated."

The most effective way to stymie a botnet is to seize those command-and-control domains to cut off communication. That's what makes a DGA such an effective weapon; companies like BitSight and Microsoft are left chasing thousands of new domains every week. But it's also how they ultimately threw up an effective roadblock. By cracking the underlying algorithm, Microsoft was able to identify the next 6,144,000 domains that Necurs was scheduled to populate over the next 25 months, and it alerted the authorities in relevant countries so they could block their registration. A court order also allowed Microsoft to seize current Necurs domains located in the US. The company is also working with ISPs around the world to identify people with infected devices and help them scrub their machines.

Other botnets, particularly Emotet, have ascended since Necurs went quiet a year ago. Crippling

Necurs still serves an important purpose, though. “Even though it is dormant, we don’t know what the possibility is of it coming on line again for nefarious purposes,” says Dahlberg.

Microsoft and its partners have ensured that if the botnet does try to mount a comeback, it won’t have very many places left to turn.

More Great WIRED Stories

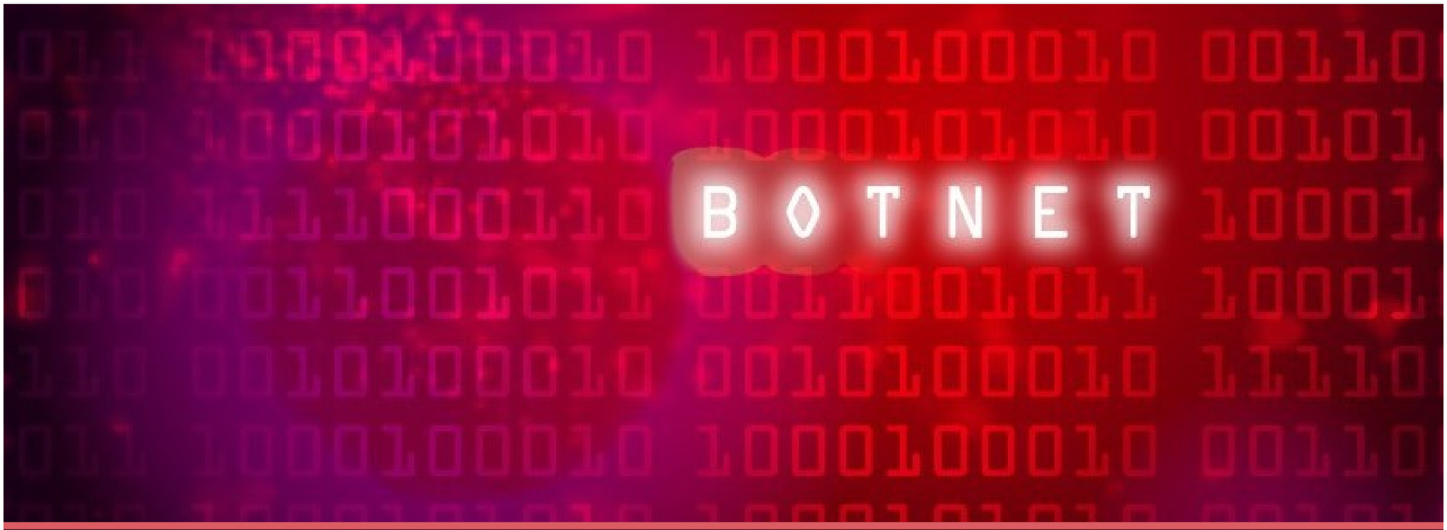
- Inside *Devs*, a dreamy Silicon Valley quantum thriller
- A fast walker gets stuck in the slow lane
- Welcome to Botnet, where everyone’s an influencer
- A hacker's mom broke into a prison—and the warden's computer
- The intricate, unintended beauty of factories and labs
- 👁 Want a real challenge? Teach AI to play D&D. Plus, the latest AI news
- 🎧 Things not sounding right? Check out our favorite wireless headphones, soundbars, and Bluetooth speakers

Brian Barrett is the digital director at WIRED, covering security, consumer technology, and anything else that seems interesting. Prior to WIRED he was the editor in chief of the tech and culture site Gizmodo and was a business reporter for the Yomiuri Shimbun, Japan’s largest daily newspaper.

DIGITAL DIRECTOR

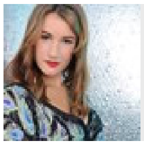
Featured Video

EXHIBIT 2



10 MAR 2020 NEWS

Necurs Botnets Busted



Sarah Coble News Writer

Eleven Necurs botnets, which infected more than nine million computers since 2012, have been severely disrupted.

The botnets were dealt a blow through the joint efforts of BitSight, Microsoft's Digital Crimes Unit (DCU), and by partners across 35 countries who today took coordinated legal and technical steps to disrupt Necurs.

The disruption was the result of years of study focused on Necurs malware, its botnets, and its command and control infrastructure. Researchers performed forensic analysis, reverse engineering, malware analysis, modules updates, infection telemetry, command and control updates, and analysis of a technique used by Necurs to systematically generate new domains through an algorithm.

“We were then able to accurately predict over six million unique domains that would be created in the next 25 months,” said a Microsoft DCU spokesperson.

The domains were reported to their respective registries in countries around the world so the websites could be blocked and prevented from becoming part of the Necurs infrastructure.

Evidence found by researchers suggests that the botnets were controlled by a single group. Of the eleven Necurs botnets discovered, four were found to be responsible for approximately 95% of all infections.

Necurs was first spotted rearing its ugly head in 2012. Over the years, the malware has been used to support a wide range of illegal activities, but its main function has been to deliver other malware.

Malicious ware dropped by Necurs has included GameOver Zeus, Dridex, Locky, and Trickbot, among others.

After infecting a system, Necurs is programmed to weaken its security to protect itself and make it easier for other malware to join the party. Using its kernel mode rootkit capabilities, the malware can disable a large number of security applications, including Windows Firewall.

Necurs botnets' activity stalled in March 2019, leaving an estimated 2 million infected systems around the world in a dormant state, awaiting revival. The year-long break was an unusually long period of inactivity for Necurs.

Describing Necurs' impact on the world, BitSight researchers wrote: "Its main uses have been as a spambot, a delivery mechanism for ransomware, financial malware and for running pump and dump stock scams.

"From 2016 to 2019, it was the most prominent method to deliver spam and malware by criminals and was responsible for 90% of the malware spread by email worldwide."

Asked how he planned to celebrate the historic botnet takedown, BitSight security researcher Valter Santos told *Infosecurity* Magazine: "BitSight will be getting back to work—we are tracking more than 200 billion events on a daily basis. There's more malware out there."

Recommended for you

Relat

Supporti
Threat Ir

US Web !

Necurs F

Bugat Ma

Necurs is

1

2

3

4

Amazon Order Confirmation Phis...

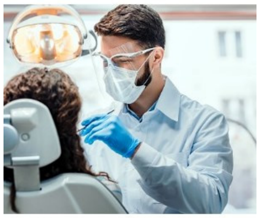
www.infosecurity-maga...

Fortinet to Pay $545,000 for Viola...

www.infosecurity-maga...

#COVID19 Fears Drive Phishing Em...

www.infosecurity-maga...



UK Dentists May Have Had Bank De...

www.infosecurity-maga...

AddThis

ALSO ON **INFOSECURITY MAGAZINE**

Garmin Outage Could Ground Aircraft

23 days ago • 1 comment

Suspected ransomware attack puts connected pilot systems out of action

Volunteer Program Aims to Secure US …

16 days ago • 1 comment

New initiative matches US election officials with volunteer cybersecurity …

Human Error Threatens Cloud …

3 days ago • 1 comment

Majority of security professionals believe human error could …

0 Comments Infosecurity Magazine 🔒 Disqus' Privacy Policy Login ▾

♡ Recommend Tweet Share Sort by Best ▾

Start the discussion…

LOG IN WITH

info security

OR SIGN UP WITH DISQUS ?

Name

Email

Password

Please access our Privacy Policy to learn what personal data Disqus collects and your choices about how it is used. All users of our service are also subject to our Terms of Service.

→

Be the first to comment.

✉ Subscribe Ⓓ Add Disqus to your siteAdd DisqusAdd ⚠ Do Not Sell My Data DISQUS

The Magazine

About Infosecurity

Subscription

Meet the Team

Contact Us

Cookies Settings

Advertisers

Media Pack

Contributors

Forward Features

Op-ed

Next-Gen Submission

EXHIBIT 3

The New York Times https://nyti.ms/337G2td

A Botnet Is Taken Down in an Operation by Microsoft, Not the Government

Employees had tracked the group, believed to be based in Russia, as it hijacked nine million computers around the world to send spam emails meant to defraud unsuspecting victims.

By David E. Sanger

March 10, 2020

WASHINGTON — Microsoft organized 35 nations on Tuesday to take down one of the world's largest botnets — malware that secretly seizes control of millions of computers around the globe. It was an unusual disruption of an internet criminal group, because it was carried out by a company, not a government.

The action, eight years in the making, was aimed at a criminal group called Necurs, believed to be based in Russia. Microsoft employees had long tracked the group as it infected nine million computers around the world, hijacking them to send spam emails intended to defraud unsuspecting victims. The group also mounted stock market scams and spread ransomware, which locks up a computer until the owner pays a fee.

Over the past year, Microsoft's Digital Crimes Unit has been quietly lining up support from legal authorities in countries around the world, convincing them that the group had seized computers in their territories to conduct future attacks.

"It's a highway out there that is used only by criminals," Amy Hogan-Burney, the general manager of the Digital Crimes Unit and a former F.B.I. lawyer, said on Tuesday. "And the idea that we would allow those to keep existing makes no sense. We have to dismantle the infrastructure."

The team struck on Tuesday, from an eerily empty Microsoft campus. Tens of thousands of workers had been ordered to stay home because the area near the headquarters in Redmond, Wash., has been a hot spot for the coronavirus. But taking down a botnet, the company concluded, was not a work-from-home task.

After cleansing the Digital Crimes Unit's command center to eliminate any live viruses, a small team of Microsoft workers gathered in a conference room at 7 a.m., flipped on their laptops and began coordinating action against another kind of global infection.

As soon as a federal court order against the Necurs network was unsealed, they began prearranged calls with authorities and network providers around the world to strike Necurs at once, cutting off its connections to computers around the globe.

"Was Mongolia hit? I think it was in the court order," one Microsoft employee asked. There was debate about Somalia — "a very last-minute win," another noted. "Tajikistan?" one person in the room asked, looking for it to turn green on a map overhead, indicating that the botnet had been neutralized there. "No joy yet."

Rapidly, they took over or froze six million domain names that Necurs was using or had inventoried for future attacks. A domain name can be a website — www.nytimes.com is a legitimate one, for example — but Necurs had created an algorithm to spawn millions of new domains, often with deceptive names, for future use against unsuspecting victims. Microsoft engineers had cracked the code.

Domain names are sold around the world, a profitable business, but Ms. Hogan-Burney said she had no illusions that the group would be permanently disabled. "We've cut off their arms, for a while," she said.

Necurs is not believed to be a state-sponsored Russian group. But intelligence officials say it is tolerated by the Russian state, and on regular occasions the Kremlin's intelligence services use private actors to pursue their goals. The Internet Research Agency, which mounted the social media disinformation campaign on Facebook and other platforms during the 2016 American president election, was a private group, though founded by a close friend of President Vladimir V. Putin of Russia.

By Tuesday's end, there was satisfaction that, for the 18th time in 10 years, Microsoft had taken down a digital criminal operation. But it was unclear whether anyone would be indicted, or even if indicted, whether they would ever face a trial.

Microsoft executives acknowledged that this was a game of whack-a-mole, and that the creators of Necurs and groups like it would be back.

“The cybercriminals are incredibly agile,” said Tom Burt, the executive who leads Microsoft’s security and trust operations, “and they come back more sophisticated, more complex. It is an ultimate cat-and-mouse game.”

The next battlefield, he said, would be the 2020 presidential election.

“We expect the volume and sophistication of the adversary attacks to accelerate as we get closer to Election Day,” he said.

“They will play many of the same moves they used in 2016,” Mr. Burt said. “But they will use others as well,” including the possibility of ransomware that locks up local voter registration systems, a major fear of election officials across the United States.

“The trick this time is to be ready, agile and aware that we have to be one step ahead,” he said.

David E. Sanger is a national security correspondent. In a 36-year reporting career for The Times, he has been on three teams that have won Pulitzer Prizes, most recently in 2017 for international reporting. His newest book is “The Perfect Weapon: War, Sabotage and Fear in the Cyber Age.” @SangerNYT • Facebook

A version of this article appears in print on March 11, 2020, Section A, Page 6 of the New York edition with the headline: Secretive Strike By Microsoft Takes Down Russian Botnet

EXHIBIT 4

Microsoft провела атаку на ботнет Necurs, подготовка которой заняла восемь лет

Microsoft помогли партнеры из 35 стран

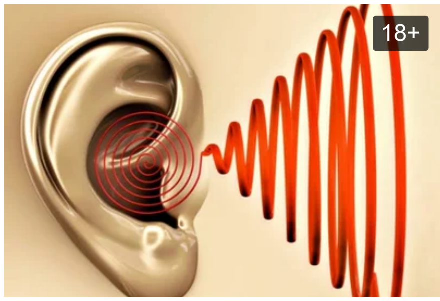
Компания Microsoft и ее партнеры из 35 стран сегодня предприняли скоординированные юридические и технические шаги, чтобы нарушить работу Necurs — одного из самых плодовитых ботнетов, который заразил более девяти миллионов компьютеров по всему миру. Атака стала результатом восьми лет отслеживания и планирования.

Напомним, ботнет - это сеть компьютеров, которые злоумышленники заразили вредоносным программным обеспечением, которое позволяет удаленно контролировать компьютеры и использовать их для совершения преступлений.

Специалисты Microsoft и их коллеги впервые наблюдали ботнет Necurs в 2012 году и смогли связать его с распространением нескольких видов вредоносного ПО, включая банковский троян GameOver Zeus. Сейчас это одна из крупнейших сетей, используемых преступниками для спама, мошенничества, атак на другие компьютеры, кражи учетных и персональных данных. Владельцы Necurs продают или сдают в аренду доступ к зараженным системами другим преступникам. На Западе считают Necurs детищем преступников из России.

В Microsoft проанализировали алгоритм, используемый Necurs для автоматического создания новых доменов, что позволило точно прогнозировать более шести миллионов уникальных доменов, которые будут созданы в течение следующих 25 месяцев. Передав эти данные в соответствующие реестры разных стран, Microsoft удалось существенно ограничить возможности роста ботнета. Неделю назад Окружной суд США в восточном округе Нью-Йорка разрешил Microsoft взять под контроль американскую инфраструктуру, которую Necurs использует для распространения вредоносных программ и заражения компьютеров-жертв. Одновременно в партнерстве с интернет-провайдерами и другими организациями по всему миру предприняты шаги, направленные на очистку компьютеров от вредоносных программ, связанных с ботнетом Necurs.

Автор: Accent | Теги: Microsoft | Источник: CDRinfo



Календарь

МАРТ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

EXHIBIT 5

Date of First Publication: March 10, 2020

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a
Washington Corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING
COMPUTER BOTNETS AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendant.

Civil Action No. 20-cv-1217

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-2 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registries associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/NECURS (http://www.noticeofpleadings.com/NECURS).

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Microsoft's attorney, Gabriel M. Ramsey at Crowell & Moring, LLP, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately.

COMPLAINT AND SUMMONS

Complaint (http://noticeofpleadings.com/NECURS/files/Complaint and Summons/Complaint.pdf)

Civil Cover Sheet (http://noticeofpleadings.com/NECURS/files/Complaint and Summons/Civil Cover Sheet.pdf)

John Doe 1 Summons (http://noticeofpleadings.com/NECURS/files/Complaint and Summons/John Doe 1 Summons.pdf)

John Doe 2 Summons (http://noticeofpleadings.com/NECURS/files/Complaint and Summons/John Doe 2 Summons.pdf)

COURT ORDERS

Order Granting TRO and Order to Show Cause re PI (http://noticeofpleadings.com/NECURS/files/Court Orders/Order Granting TRO and Order to Show Cause re PI.pdf)

Order Granting Motion to Seal (http://noticeofpleadings.com/NECURS/files/Court Orders/Order Granting Motion to Seal.pdf)

Order Granting Doe Discovery (http://noticeofpleadings.com/NECURS/files/Court Orders/Order Granting Doe Discovery.pdf)

Order Granting Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Court Orders/Order Granting Preliminary Injunction.pdf)

APPLICATION FOR EMERGENCY TEMPORARY RESTRAINING ORDER (TRO) AND PRELIMINARY INJUNCTION

Application for TRO and Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Application for TRO/Application for TRO and PI.pdf)

Brief In Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Application for TRO/Brief ISO of Motion for TRO & PI.pdf)

Proposed Order re TRO and Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Application for TRO/Proposed Order.pdf)

Lyons Declaration in Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Application for TRO/Lyons Declaration.pdf)

Ghaffari Declaration in Support of Motion for TRO and Preliminary Injunction (http://noticeofpleadings.com/NECURS/files/Application for TRO/Ghaffari Declaration.pdf)

MOTION FOR ORDER TEMPORARILY SEALING DOCUMENTS

Application for Leave to Seal (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Application for Leave to Seal.pdf)

Motion to Seal (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Motion to Seal.pdf)

Brief in Support of Motion to Seal Documents (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Brief ISO of Mtn for PO Termp Sealing Docs.pdf)

Ramsey Declaration in Support of Motion to Seal Document (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Ramsey Dec ISO Motion to Seal.pdf)

Proposed Order re Motion to Seal (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Proposed Order to Seal.pdf)

March 10, 2020 Notice of Execution of Ex Parte Temporary Restraining Order and Notice re Unsealing of Case (http://noticeofpleadings.com/NECURS/files/Motion for Order Temporarily Sealing Documents/Dkt. 12_Notice of

Exceution and Motion to Unseal.pdf)

MISCELLANEOUS

Contact Us

If you wish to contact us by e-mail, fax, phone or letter please contact us at:

Gabriel Ramsey
Crowell & Moring LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Telephone: +1 (415) 365-7207
Facsimile: +1 (415) 986-2827
Email: gramsey@crowell.com (mailto:gramsey@crowell.com)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. 20-CV-1217 (LDH)

CERTIFICATE OF DEFAULT

I, Douglas C. Palmer, Clerk of the Court of the United States District Court for the Eastern District of New York, do hereby certify that the docket entries in the above captioned action indicate that a Complaint was filed on March 5, 2020 and that service was made on Defendants John Does 1-2 on March 11, 2020 and March 30, 2020, by email and publication as authorized by the Court in the Temporary Restraining Order And Order to Show Cause re Preliminary Injunction entered on March 5, 2020 and in the Preliminary Injunction entered on March 31, 2020.

I further certify that the docket entries indicate that Defendants John Does 1-2 have not filed any answer or otherwise moved with respect to the Complaint herein.

Dated:

DOUGLAS C. PALMER, Clerk of the Court

By:________________________________