


CLERK OF DISTRICT COURT
U.S.D.C. - Atlanta

NOV 14 2017

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

MICROSOFT CORPORATION

Plaintiffs,

v.

**JOHN DOES 1-51,
CONTROLLING MULTIPLE
COMPUTER BOTNETS
THEREBY INJURING
MICROSOFT AND ITS
CUSTOMERS**

Defendants.

CASE NO.

1:17-CV-4566

FILED UNDER SEAL

**DECLARATION OF RODELIO G. FIÑONES IN SUPPORT OF
MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE*
TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW
CAUSE RE: PRELIMINARY INJUNCTION**

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

NOV 14 2017

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

MICROSOFT CORPORATION

Plaintiffs,

v.

**JOHN DOES 1-51,
CONTROLLING MULTIPLE
COMPUTER BOTNETS
THEREBY INJURING
MICROSOFT AND ITS
CUSTOMERS**

Defendants.

CASE NO.

1:17-CV-4566

FILED UNDER SEAL

**DECLARATION OF RODELIO G. FIÑONES IN SUPPORT OF
MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE*
TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE
RE: PRELIMINARY INJUNCTION**

I, Rodelio G. Fiñones, declare as follows:

1. I am a Senior Researcher in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs group. I make this declaration in support of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction. 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 discussed in this declaration.

I. Introduction

2. I have been employed by Microsoft since June 2009. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. I am the lead researcher in the Digital Crimes Unit focusing on different categories of malware, including botnets. In such capacity, I research emerging malware threats through analysis of submitted samples, reverse engineering, forensic examination, data stream analysis, and development of tools to track botnet development. I also work closely with the Microsoft team responsible for developing malware prevention and eradication tools. Prior to joining Microsoft, I worked for Fortinet Technologies (Canada), Inc. as a Principal Software Developer/Researcher (2007–09) and a Senior Antivirus Analyst (2004–07). My job responsibilities included research and analysis of complex malware and development of tools to detect and eradicate malware. From 1999–2004, I worked for Trend Micro, Inc. as a Senior Antivirus Researcher and Antivirus Engine Developer. During my professional career, I have received advanced, specialized training and extensive practical experience in investigating malware and botnets and in devising technical countermeasures to detect and disable

them. A true and correct copy of my curriculum vitae is attached to this declaration as **Exhibit 1**.

3. Currently, I am a member of a team actively investigating a family of botnets associated with the Gamarue malware (also known as “Andromeda” or “Wauchos” malware, as explained in paragraph 15, below). In preparation of this declaration, I reviewed the declaration of Co-Microsoft declarant Vishant Patel and the declaration of Jean-Ian Boutin, an analyst from ESET, spol. s r. o., an antivirus company, concerning Gamarue. I agree with the content in both these declarations, and it has confirmed my own conclusions regarding the Gamarue malware.

4. In this declaration, I will explain how the Gamarue malware was identified by Microsoft, how this malware operates and spreads itself to the computers of Microsoft and its customers, and how it harms Microsoft and its customers.

II. Microsoft’s Antivirus Products and Services

5. Microsoft provides antivirus products and services to its customers, including Windows Defender, Forefront Endpoint Protection, and Microsoft Security Essentials, among others. These products and services operate in conjunction with Microsoft customer computers to detect malware activity, such as a particular malware infection, that threatens the computers. For customers who

elect to provide samples to Microsoft, an optional reporting feature called the Microsoft Active Protection Service (“MAPS”) is built into these antivirus products and services for collecting information about malware operating on customer computers. Upon encountering malware activity, information about the malware is reported to the Microsoft Malware Protection Center (“MMPC”) through the MAPS.

6. The MMPC analyzes malware information received from the customer computers for intelligence to be used for mitigating future malware threats. This intelligence can include information identifying specific malware types and strains encountered on the customer computers, the general locations of the computers, and a timestamp indicating the date and time of the encounter.

7. In certain instances, the MMPC runs the malware in a secure environment to further study its behavior and determine intelligence for mitigating future malware threats. Based on this analysis, signatures and suspicious-behavior patterns may be developed and provided to the Microsoft antivirus products and services so that they are more effective at combatting the malware threat on customer computers.

8. Beginning in 2011 when Microsoft first detected Gamarue, Microsoft’s investigation into the Gamarue malware began by analyzing the data it was receiving via the MAPS reporting feature. Microsoft determined that a significant number of

malware encounters involved Gamarue. Subsequently, Microsoft began investigating the Gamarue architecture, design, and functions. This investigation included infecting several researcher-controlled computers with the Gamarue malware so that researchers could monitor all of the illicit communications going to and coming from the infected computers, as well as analyze the activities of the infected computers. Based on this investigation, Microsoft determined the information described herein. Some of the information provided below overlaps with the information provided by Vishant Patel in his declaration it is included only to provide context to my conclusions.

III. The Gamarue Malware

A. Botnet Infrastructure

9. When a computer is infected with the Gamarue malware, it becomes part of a “botnet.” A botnet is a collection of individual computers, each running malware that allows communications between the infected computers and one or more server computers controlled by the distributor of the malware, typically referred to as the “command and control” servers (“C2 servers”), as shown in **Figure 1**, below. In **Figure 1**, the malware infected red computers are controlled by a cybercriminal through the C2 server. The blue lines represent Internet communications between the infected victim computers and the C2 server.

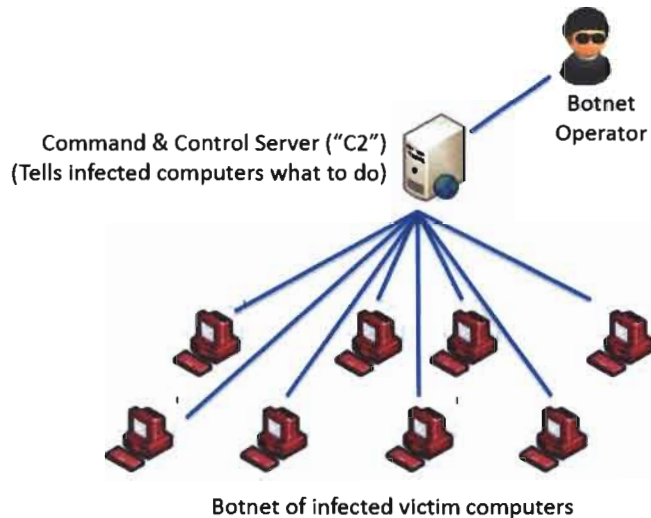


Fig. 1

10. Through the C2 server computer or computers, cybercriminals, frequently referred to as “bot herders” or “botnet operators,” are able to control the infected computer, steal information from the infected computers, provide instructions or additional malware modules to the infected computers, and upload data from the infected computers. Cybercriminals often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them.

11. Botnets provide a very efficient means of controlling large numbers of computers and targeting any action internally against the contents of those computers or externally against other computers on the Internet. The third parties running the botnet can use the network of infected personal computers for various

nefarious activities including spam, denial of service attacks on other computers connected to the Internet, theft of financial and banking data, eavesdropping, stalking, and other schemes. Access to the compromised personal computers can also be sold, rented, leased, or swapped by one criminal group to another.

12. The Gamarue botnet consists of two tiers: the infection tier and the command and control tier. The infection tier is comprised of infected personal computers owned by innocent and unsuspecting people. These personal computers are sometimes referred to as “bots.” These might be office or home desktop computers, laptop computers, computers in public libraries, computers located on Microsoft’s campus, and so forth. Computers can become infected in one of several ways. A person may use an infected thumb-drive borrowed from a friend or colleague that contains the malware; access a malicious link or compromised website on which the malware downloader is staged (including social media sites like Facebook, Twitter, and Skype); or download other malware containing instructions to download Gamarue. For example, a victim might receive a Facebook message that appears to be from a friend or family member, but is really sent from one of the Defendants. The post will include a link —when the victim clicks on the link, the Gamarue malware is secretly downloaded to the victim’s computer.

13. Once a computer is infected with the Gamarue malware, the malware will instruct the computer to contact the botnet controller's C2 server over the Internet. The means by which an infected computer contacts a C2 server is discussed in detail in the Patel Declaration. C2 servers refer to either physical server computers or software running on computers that support the Gamarue botnets. Defendants use and control these C2 servers to continuously control the Gamarue-infected computers.

14. **Figure 2** below provides a schematic overview of how the Gamarue botnet ecosystem operates.

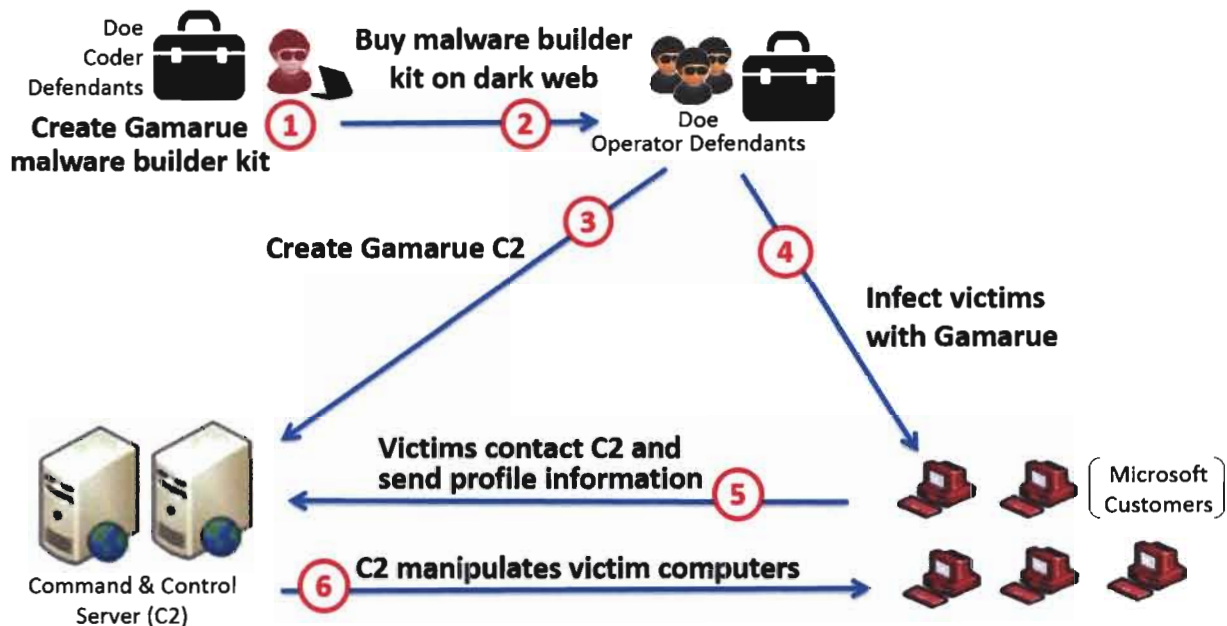


Fig. 2

- a. Step One: The Coder Defendants develop the Gamarue malware and offer it for sale in a malware builder kit.
- b. Step Two: The Operator Defendants acquire the builder kit from the Coder Defendants and use it to create and operate a Gamarue botnet, as shown in steps 3–6.
- c. Step Three: The Operator Defendants create a series of C2 servers, which act as the infrastructure for the botnet. Microsoft has detected at least 464 Gamarue botnets utilizing at least 1,214 domain addresses over time.¹
- d. Step Four: The Operator Defendants infect the Microsoft Windows operating system on victim computers with the Gamarue malware.
- e. Step Five: Upon infection, the Gamarue malware causes the victim computers to contact the C2 servers to provide information about the victim computers. This information includes a volume serial number for the victim computer (this is used as a bot ID for the computer), the Gamarue version with which the computer has been infected, the operating system that is running on the victim computer, the local IP address for the victim computer, an indication as to whether the victim account has administrative rights on the victim computer, and the keyboard language setting for the victim computer.

¹ Not all 1,214 domains are currently active.

f. Step 6: The Operator Defendants use the C2 servers to manipulate the victim computers by communicating with the Gamarue malware on the infected computers. As will be discussed in more detail below, criminal actors like the Operator Defendants primarily use the Gamarue malware to load at least 80 additional types of malware onto victim computers. This expands the scale of crimes committed against unsuspecting computer owners and on the public at large. Defendants can also use the Gamarue C2 servers to download, install, or remove additional plugins; update the Gamarue malware program; uninstall the Gamarue malware; spy on the victim by capturing keystrokes and mouse actions and viewing the victim's desktop; capture any data (e.g., credentials) submitted by a victim online; and turn the computer into a proxy server for serving malware to other computers on the Internet. Most if not all owners of Gamarue-infected computing devices are unaware that their machines are infected and operating as part of the Gamarue botnets.

15. The Gamarue malware is also known as "Andromeda" or "Wauchos." Companies and researchers involved in malware analysis and prevention frequently use different names or labels to refer to the same family of malware. In other words, Gamarue, Andromeda, and Wauchos are three different expressions or strains of the same malware, because they share common underlying code.

16. All of the above described acts are carried out without authorization from Microsoft or the owners and operators of the infected computers.

B. Gamarue is Available as a “Crime Kit” for Download

17. The Gamarue crime kit includes a Gamarue builder tool that has certain built-in functionality. It also includes several different plugins, some of which are part of the standard crime kit, and some of which are available for an additional cost. Thus, the Coder Defendants monetize the crime kit through plugin purchases by the Operator Defendants. The Defendants employ the Gamarue crime kit and associated plugins, as described below, without authorization from Microsoft or the operators of the infected computers.

18. There are numerous commands that are built into the Gamarue builder kit and can be issued as a task from a C2 server. These commands are:

- Download Command: Downloads additional malware onto the infected machine;
 - Install Plugin: Downloads and installs additional plugins onto the infected machine;
 - Update Bot: Updates the Gamarue malware program;
 - Uninstall Plugin: Removes a Gamarue plugin from the infected machine;
- and

- Uninstall Bot: Removes evidence of Gamarue presence from the infected machine.

19. In addition to the built-in functionality, several different plugin functionalities are available for Operator Defendants to purchase and install on victim computers, including the following:

- Keylogger: Captures all keystrokes and mouse actions on the infected machine, which facilitates stealing passwords, login information, financial information, etc.;²
- Formgrabber: Captures any data (e.g., login credentials) submitted by a victim when online—this plugin targets Chrome, Firefox, and Internet Explorer;³
- Rootkit: Surreptitiously injects into all running processes, which gives Gamarue persistency on the infected machine;⁴
- Sock5: Turns the infected machine into a proxy server for serving malware and malicious instructions to other computers on the Internet;⁵
- TeamViewer: Enables remote control, spying on a victim's desktop, and

² Coder Defendants reportedly advertise the Keylogger plugin for \$150.

³ Coder Defendants reportedly advertise the Formgrabber plugin for \$250.

⁴ Coder Defendants reportedly make the Rootkit plugin available for free.

⁵ Coder Defendants reportedly make the Sock5 plugin available for free.

file transfer;⁶ and

- USB Spreader: Provides capability to spread Gamarue malware itself via removable drives (for example, portable hard drives or flash drives connected via a USB port).

20. Several of the functionalities mentioned above enable Gamarue to resist countermeasures. First, Gamarue installs itself at the deepest layers of Windows, and will conceal itself on the user's computing device by hiding its files and making changes to the Windows Registry.

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\taskmgr.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\

21. Additionally, various functions enable the botnet operator to uninstall plugins, or even uninstall the Gamarue malware, altogether, thus covering the Defendants' tracks. Furthermore, Gamarue surreptitiously tampers with the operating systems of infected computers by disabling Firewall, Windows Update, and User Account Control functions on all versions of Windows, other than

⁶ Coder Defendants reportedly advertise the TeamViewer plugin for \$250.

Windows 10—this functionality cannot be re-enabled until the Gamarue infection has been removed from the infected computer. **Figure 3**, below, shows messages the infected computer victims receive from the Windows operating system when Gamarue surreptitiously eliminates security protections.



Fig. 3

Victims have no recourse to change these settings, and they may incorrectly hold Microsoft's Windows operating system responsible for the problems caused by Gamarue. Even with professional assistance, it can be very difficult for victims to clean an infected computer.

22. Gamarue has also deployed certain countermeasures that prevent analysis by researchers and law enforcement. For example, prior to infection, Gamarue checks a pre-compiled list of the processes running on a potential victim's machine and, if the machine is found to be running a process that may be associated with researchers or law enforcement (e.g., processes related to virtual machines or sandboxing), Gamarue will not infect that machine.

23. Other functionalities mentioned above permit a botnet operator to spy on victims' online activities. For example, both the Keylogger and Formgrabber plugins facilitate the theft of usernames and passwords. This stolen information is transferred to the C2 server, where the botnet operator can collect it for later use. Additionally, the TeamViewer plugin enables remote control, spying, and file transfer by the Defendants.

24. Gamarue includes a control dashboard functionality, depicted in the illustration in **Figure 4**, below, that allows Operator Defendants to easily inflict all of the above operations on multitudes of infected computers.

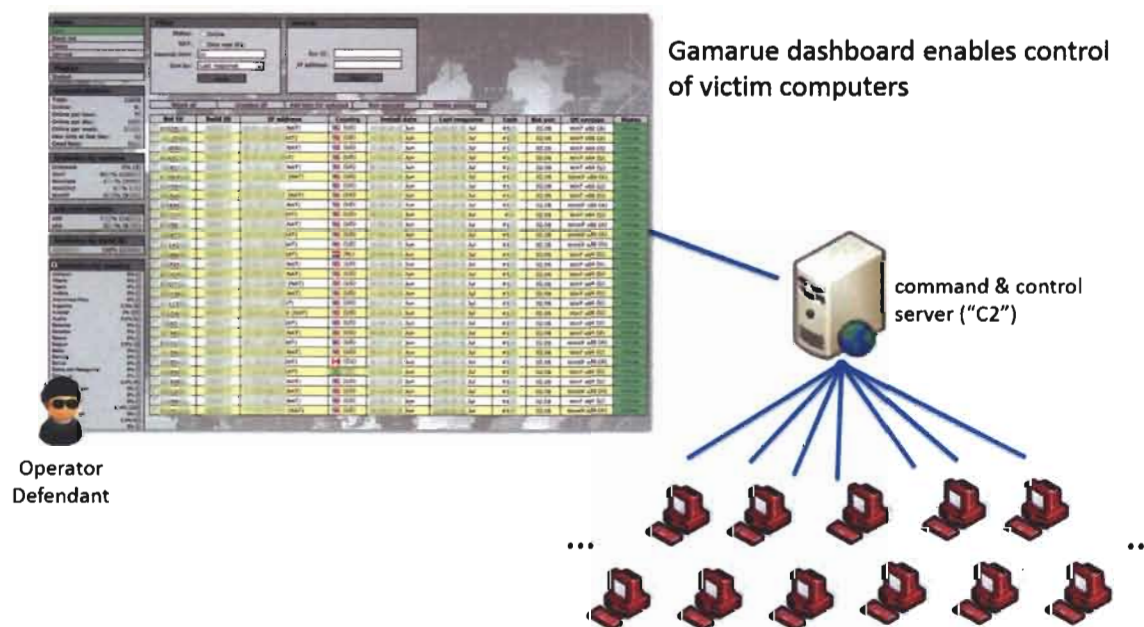


Fig. 4

An Operator Defendant simply selects infected computers from the dashboard and directs malware downloads or other malicious instructions to them through the C2 server.

C. Gamarue Exposes Infected Computers to Additional Malware

25. Criminal actors, like the Defendants, primarily use the Gamarue malware to load at least 80 additional types of malware onto victim computers. This additional malware increases the scope of harm that is inflicted on unsuspecting computer owners and the public at large. This “devil’s brew” of malware includes dropping ransomware onto Gamarue infected computers, which then spreads the ransomware to a victim’s computer until ransom is paid, denial of service attacks that flood legitimate sites on the Internet with web traffic that renders them inoperable, and password stealers that collect victims’ banking credentials. The additional malware can be categorized into ten different families of malware:

- **Backdoor**: This malware facilitates bypassing normal computer security and authentication features, thereby granting cybercriminals unauthorized remote access to a victim’s computer.
- **DDoS**: Distributed Denial of Service (“DDoS”) malware is used to carry out a type of cyberattack called a Denial of Service (“DoS”) attack. This involves using multiple compromised systems (e.g., infected computers in

a botnet) to simultaneously target a single computer system. For example, a botnet herder can cause all of the infected computers in his botnet to simultaneously flood the target computer system with requests, thereby overloading the target computer system and making it impossible for the target computer system to respond to legitimate requests. This effectively shuts down the target computer system. For example, a DDoS attack may be used against a government computer system to shut it down and prevent legitimate users from accessing it.

- Password stealing: This malware typically lies dormant on a victim's computer until the victim accesses a website (or other secure resource) that requires providing user credentials, such as when the victim navigates to a bank website. Then the malware steals the victim's credentials and sends the credentials to cybercriminals.
- Ransomware: This malware installs covertly on a victim's computer and then secretly encrypts the victim's files, including photos, documents, and others. This encryption blocks the victim's access to the files. The victim is then notified, and payment is demanded in order to decrypt the files. Many times, even after the victim has paid the ransom, the victim's files are left encrypted and are thus permanently lost.

- Spammer: This malware uses a victim's computer to send unsolicited bulk messages ("spam") to other computers. These messages often include links to nefarious websites, contain malware or other potentially harmful content, or promote fraud or other schemes. In many cases, the victim's computer appears as the sender of the spam.
- Trojan: A trojan (or "Trojan horse") is a type of malware that misleads a victim (or the victim's computer) with respect to its true nature. For example, trojan malware can be disguised as legitimate software.
- Trojan downloader: This is a special type of trojan malware that secretly downloads and installs malware onto a victim's computer. The trojan downloader tricks a victim into believing that legitimate data or software is being downloaded (e.g., an email attachment or video codec update).
- VirTool: This category includes many different programs that are used by other malware in order to facilitate the operation of the other malware (e.g., an obfuscator that aids malware in evading detection by security software on a victim's computer).
- Worm: This malware replicates itself in order to spread the infection to other computers.

- Unknown: This category encompasses malware that has been detected by Microsoft, but that has not yet been identified or classified.

26. Because the Gamarue malware is used to load these additional families of malware onto victims' computers, the Gamarue malware exposes victims to all of the harms outlined above. Additionally, other malware has undoubtedly been distributed using Gamarue which has not yet been discovered, and the resulting harm would continue unless customers can be alerted.

IV. Gamarue Damages its Victims in Multiple Ways

A. Gamarue Damages Infected Computers and Microsoft Software

27. The installation of the Gamarue malware, in and of itself, damages the victim's computer, the Windows operating system, and the applications on victim's computer, because Gamarue makes changes at the deepest and most sensitive levels of an infected computer's operating system, including the kernel, registry, and system files. Additionally, the Gamarue plugins discussed above allow Defendants to spy on victims and steal passwords and other valuable information, among other harmful activities. The Gamarue malware also exposes infected computers to the additional malware, exposing victims to additional harms.

28. Victims are usually unaware of the fact that their computing devices are infected and have become part of a Gamarue botnet. Many victims of Gamarue will

never learn that they are infected, or, if they do determine that they are infected, they will have a very difficult time in removing the infection and in restoring the security features of their computers. Even with professional assistance, cleaning an infected computer can be exceedingly difficult, time-consuming, and frustrating.

B. Gamarue Damages Microsoft's Reputation, Brands, and Goodwill

29. In addition to the harm inflicted on individual victims and their infected computers, Gamarue also irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill.

30. Microsoft® is a provider of the Windows® operating system, the Internet Explorer® browser, and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing strong and famous world-wide symbols that are well recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, Internet Explorer®, and other marks. Copies of Microsoft's trademark registrations are provided as **Appendix B** to the Complaint.

31. The Gamarue malware physically alters and corrupts the products that Microsoft owns and licenses to its customers, such as the Windows operating system. The Windows operating system is owned by Microsoft and licensed to its users. Attached as **Appendix C** to the Complaint are true and correct copies of end-user license agreements for Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2000, Windows 8, Windows Server 2008, and Windows 10, all of which are specifically targeted by Gamarue. In effect, once infected, altered, and controlled by the Coder Defendants or Operator Defendants (collectively, the “Defendants”), the Windows operating system, as described above, ceases to operate normally and becomes a tool for Defendants to conduct their theft. Yet the Windows operating system continues to bear the Microsoft Windows trademark. This is intended to, and does, mislead Microsoft’s customers into believing the Windows operating system is functioning normally. These alterations and corruptions are carried out without the authorization of Microsoft or its victimized customers that own the infected computers.

32. The Formgrabber plugin surreptitiously installs on an infected computer at the direction of a Defendant and attaches to the Internet Explorer browser without authorization from Microsoft or its customers that license Internet Explorer from Microsoft for use on their computers. Once installed, the Defendants

use the Formgrabber to siphon off information that the infected computer owner enters into Internet Explorer. This may include usernames and passwords for online accounts, such as email and banking institution accounts. Yet the Internet Explorer browser continues to bear Microsoft's Internet Explorer trademark. This is intended to, and does, mislead Microsoft's customers into believing that Internet Explorer is functioning normally, when in reality it is surreptitiously augmented by the Formgrabber plugin.

33. In my experience, malware infections tarnish the reputation of Microsoft and its products, because consumers often incorrectly attribute to Microsoft the negative impact of Gamarue and any additional malware downloaded to their computing devices as a result of the Gamarue malware. This injures Microsoft and its reputation, brand, and goodwill and creates a serious risk that customers may abandon Microsoft's products. Once customers abandon Microsoft's products, there are significant challenges to winning back such customers, given the cost the customers bear to switch to new products and perceived risks based on their negative experiences with the Microsoft products that were adulterated by Gamarue.

34. Microsoft has devoted significant computing and human resources to investigating Gamarue malware infections and helping customers determine

whether or not their computing devices are infected, and, if so, cleaning them. These efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Furthermore, Microsoft must also incorporate security features into its Windows operating system in an attempt to prevent Gamarue infections and combat the harm caused by the Gamarue malware.

35. Microsoft has observed and is aware of situations in the past in which even a hint of action against the infrastructure of cybercriminals resulted in the cybercriminals changing or moving their operations to avoid detection, which nullified all prior investigations and required investigators to restart their efforts from scratch. This evasive action by the cybercriminals prevented mitigation of the harm caused to the public and resulted in the destruction of evidence important to proving a claim. Any advance notice to the Defendants here will likely lead to this type of nullifying action and require Microsoft to restart its investigation of Gamarue from scratch—an investigation which has taken over 22 months to complete. During this time, the above-described harm to Microsoft, its customers, and the public at large will be ongoing.

///

///

I declare under the 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 13th day of November, 2017.



Rodelio G. Finales

Rodelio G. Fiñones

Objective:

To acquire a rewarding career in the field of computer and internet security where my expertise, experience, and knowledge in malware security will be utilized to contribute to the success of the company.

PROFESSIONAL EXPERIENCE:

Senior Software Engineer, Digital Crimes Unit (Nov 2017 – Present)

Microsoft

- Design and develop tools and automation projects for unpacking and tracking botnets.
- Utilize big data (cosmos) to analyze malware treat landscape and to better protect the customer.
- Collaborate with other DCU investigators to research on prevalent malwares for CME (MS Collective Malware Eradication) to disrupt/eradicate malwares.
- Maintain and improve the malware crawlers and sinkhole systems.

Senior Antivirus Researcher / Strategist (June 2009 – Nov 2017)

Microsoft

- Handle malware samples from different sources to provide analysis, tracking, detections, advice, and remediation.
- Tracking top acute threats impacting customer and doing end to end research and providing up to date protection and mitigation (Ex: Zeus/Zbot, Locky, Cerber, etc.)
- Lead the team on focus research of different categories of malwares such Botnets, Clickfraud, MSIL, and Spambots to provide different kind customer protection such as sourcing, protections (File, memory, and cloud-based, behavior-based, and etc.). Also includes identifying the malware infection chain and monetization.
- Design and develop tools and automation projects for unpacking and tracking botnets.
- Utilize big data (cosmos) to analyze malware treat landscape and to better protect the customer.
- Lead team and hands on research on prevalent malwares for CME (MS Collective Malware Eradication) to disrupt/eradicate malwares.
- End to end research and development of antimalware engine and product features to improve customer protections.
- Drive improvements to windows platform and its components (OS, script engines – JS, PS, etc.)
- Static and dynamic analysis of different types of malwares and vulnerabilities.

- Creating rules and programs to improve automatic detections of malwares.
- Respond to malware outbreaks.
- Write tweets, blogs, research papers, and present to top security conferences.
- Provide mentoring to other researchers.

Principal Software Developer / Researcher (Dec 2007 – June 2009)

Fortinet Technologies (Canada), Inc.

- Improved signature-based detection algorithm to support more complex malwares. Detection methods such as x-raying and behavioral and characteristics detections.
- Research and develop AV engine features to support packer through script-based. Generic unpacker coupled with script-based unpacker will be a powerful and effective solution for most malwares.
- Handle complex malwares analysis and detection through script-based or hard-coded.
- Improvements and optimizations for Fortinet's AV detection algorithms.
- Provide technical knowledge to new AV analyst.

Senior Antivirus Analyst / Engine developer (May 2004 – Dec 2007)

Fortinet Technologies (Canada), Inc.

Analysis, Research and Development Projects

- Research, design, and develop the clean engine for Fortinet's desktop Antivirus product. It supports cleaning Win32 PE, Office, DOS, and script formats.
- Improve the scanning technology through research and development of new scanning algorithm that suits for complex viruses.
- Fix bugs and AV scan and clean engine limitations
- Participate in the research, development, and improvements of Win32 emulator engine.
- Create detection module for hard to detect viruses such metamorphic, polymorphic, and EPO viruses.
- Improved the scanning technology for scripts malwares.
- Research, design, and develop an automated system to replicate, analyze, and heuristically detect known and unknown malwares through sandboxing technology.
- Handle complex malwares.
 - Analysis
 - Creating detection signatures
 - AV Engine support (if necessary)

Other Tasks:

- Provide malware related technical expertise to analyst and product development team.
- Create documentation for developed systems.
- Conduct trainings regarding virus analysis, detection and disinfection algorithm.
- Provide quick and quality solution to customer problems.
- Configure replication system for any kinds of malware

Senior Anti-Virus Researcher / AV Engine Developer (Nov 1999 – April 2004)
Trend Micro, Inc. (Anti- Virus and Internet Security)

AV Trainee

- 3-month extensive virus / malware training. Include analysis and creation of detection and clean signatures.

AV Technical Support Engineer

- Provides complete solution to the customer.
 - Provides scan and clean solution. Includes signature to remove system infections such as registry, system files, process, services, and files.
 - Create detailed / comprehensive virus description and manual removal instructions.
 - Provides other assistance needed by the clients.

AV Research Engineer

- Focus on the detailed / comprehensive analysis of Windows viruses.
- Process escalation cases from Virus support engineers.
- Conduct technology upgrade trainings to Virus support team (New virus technology; new Scan / Clean feature).
- Respond to Virus Alerts
- Develop removal tools for specific malware.
- Design and develop TSC (Trojan System Cleaner). Engine module to detect and restore system infection through registry, process, system files, and services.
- Process Scan / Clean Engine related cases.
- Analyze exploits and system vulnerabilities (Windows & Linux).
- Research and develop a system for automating the replication of malware that covers controlled and simulated Internet environment
- Research and develop Scan/Clean Engine modules:
 - Metamorphic virus support
 - Win32 virus clean modules
 - New file formats support
 - Trojan System Cleaner
 - Compression / Packer engine support (UPX, Petite, and PEPack)

Extra

- Develop a network scanner tool that runs in either a gateway mode or as personal IDS. This is a company-wide contest and we were able to get in the final 6 out of 15 contestants.

TECHNICAL SKILLS:

- Advance knowledge and experience in reverse engineering any kinds of malware using debugger (Soft-ice, IDA Pro, OllyDbg, and Immunity debugger)
- In-depth knowledge and experience in exploits and vulnerabilities.
- Strong knowledge and experience in creating comprehensive virus description.
- Strong experience in developing detection and cleaning engine for different kinds of malware such as virus, worms, Trojans, and spywares.
- In-depth knowledge in windows operating system internals.
- In-depth knowledge and experience in virus, Trojans, worms, and spywares behaviors.
- Experience in TCP/IP networks, Unix/Linux networks (AIX, Redhat, Slackware, Ubuntu), Windows network (Windows 9X/NT/2K), Novell Netware. Background knowledge in Windows CE, Palm, and EPOC operating system.
- Advance experience in C and DOS/Win32 Assembly, VB Script, JavaScript.
- Experience in C++, Linux shell scripts, PowerBuilder, and SQL programming.
- Intermediate experience in analyzing and testing various Anti-virus products.
- Experience in using soft-ice debugger, IDA Pro, OllyDbg, Snort, and Ethereal.
- Intermediate knowledge in network protocols like TCP/IP, IPX/SPX, SMTP, FTP, HTTP, DNS, NTTP, and MAPI32.
- Intermediate knowledge in Windows and Unix/Linux system and network security.
- Knowledge in ASP, MS Access, FoxPro, and HTML.
- Knowledge in IP chains/tables, Ethereal packet sniffer, Snort IDS, Tripwire integrity checker.
- Knowledge in Lotus Notes and Domino server
- Have a strong problem-solving ability, reliability, team player and hard working.
- Experience in python and Django web framework.

PREVIOUS EMPLOYMENT:

System analyst / Programmer (July 1999, October 1999)

Gestalt Consulting Inc. (PowerBuilder and MS SQL)

- Create, maintain, and improve Inventory system and Accounting system.
- Provide support to problem of clients.
- Review and document the current application system.

EDUCATION:

Bachelor of Science in Computer Engineering (1995 -1999)

East Asia College of Information Technology, May 1999, 3.2/4.0 GPA

Secondary Education (1991 - 1995)

Gregorio Perfecto High School

Primary Education (1985 – 1991)

Magat Salamat Elementary School