Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andromeda)

blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/

December 4, 2017

Today, with help from Microsoft security researchers, law enforcement agencies around the globe, in cooperation with Microsoft Digital Crimes Unit (DCU), announced the disruption of Gamarue, a widely distributed malware that has been used in networks of infected computers collectively called the Andromeda botnet.

The disruption is the culmination of a journey that started in December 2015, when the Microsoft Windows Defender research team and DCU activated a Coordinated Malware Eradication (CME) campaign for Gamarue. In partnership with internet security firm ESET, we performed in-depth research into the Gamarue malware and its infrastructure.

Our analysis of more than 44,000 malware samples uncovered Gamarue's sprawling infrastructure. We provided detailed information about that infrastructure to law enforcement agencies around the world, including:

- 1,214 domains and IP addresses of the botnet's command and control servers
- 464 distinct botnets
- More than 80 associated malware families

The coordinated global operation resulted in the takedown of the botnet's servers, disrupting one of the largest malware operations in the world. Since 2011, Gamarue has been distributing a plethora of other threats, including:

- Petya and Cerber ransomware
- Kasidet malware (also known as Neutrino bot), which is used for DDoS attacks
- Lethic, a spam bot
- Info-stealing malware Ursnif, Carberp, and Fareit, among others

A global malware operation

For the past six years, Gamarue has been a very active malware operation that, until the takedown, showed no signs of slowing down. Windows Defender telemetry in the last six months shows Gamarue's global prevalence.

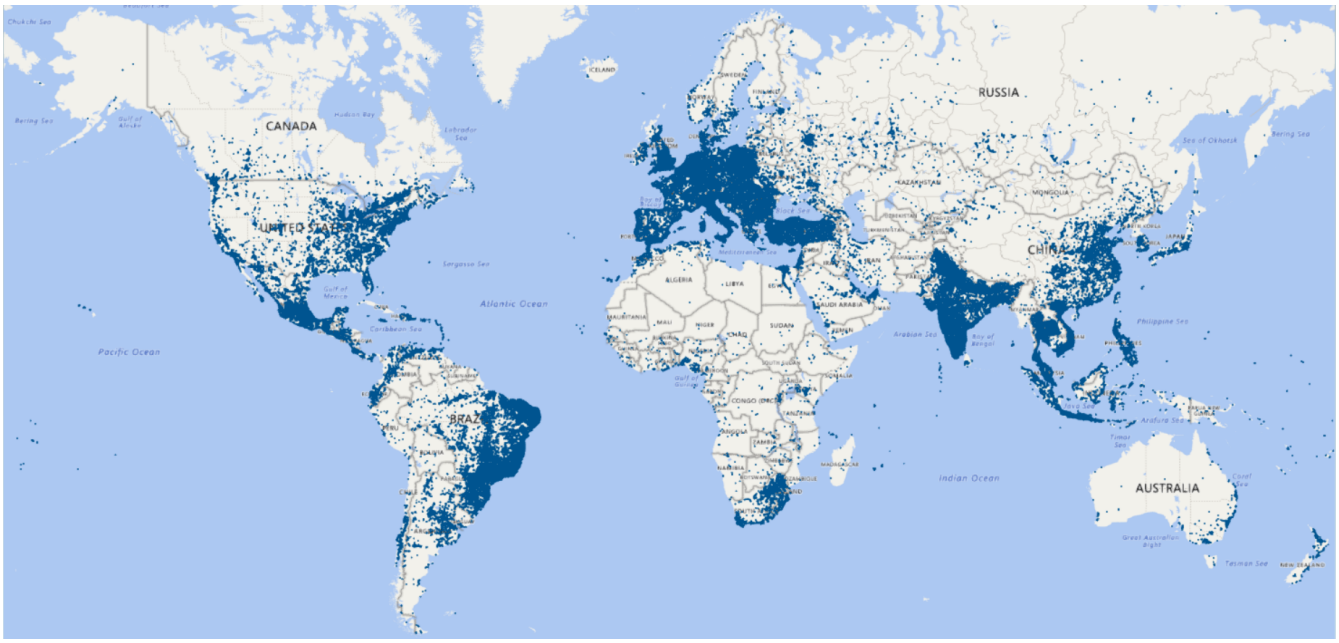

Figure 1. Gamarue's global prevalence from May to November 2017

While the threat is global, the list of top 10 countries with Gamarue encounters is dominated by Asian countries.

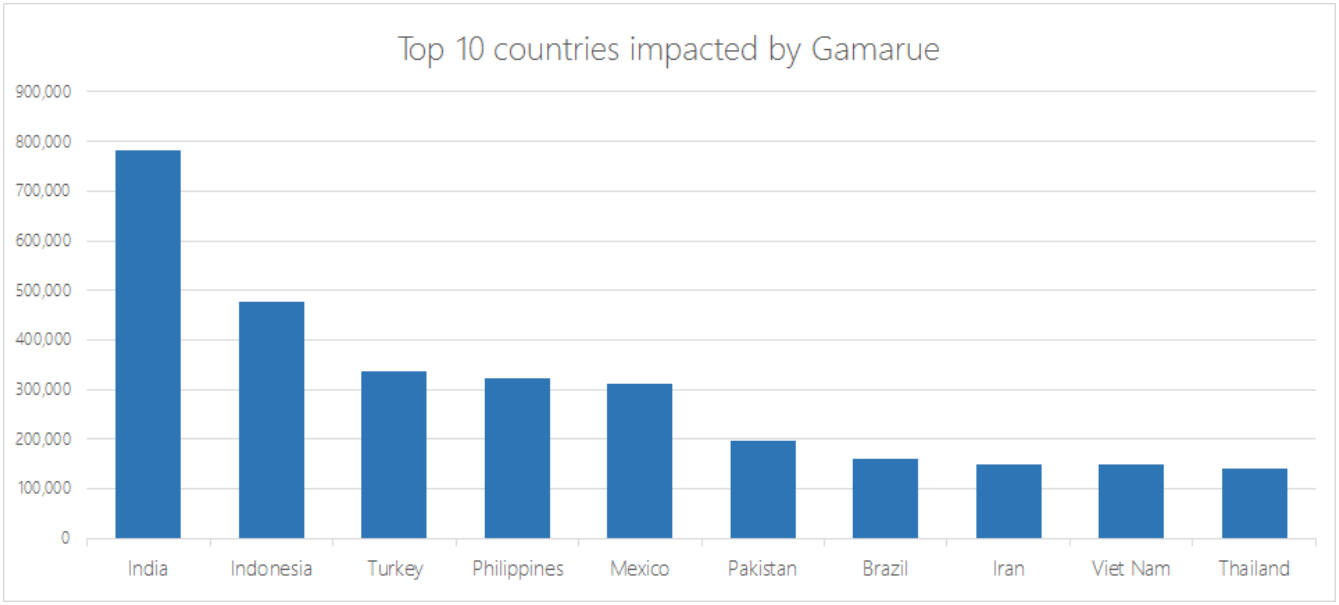

Figure 2. Top 10 countries with the most Gamarue encounters from May to November 2017

In the last six months, Gamarue was detected or blocked on approximately 1,095,457 machines every month on average.

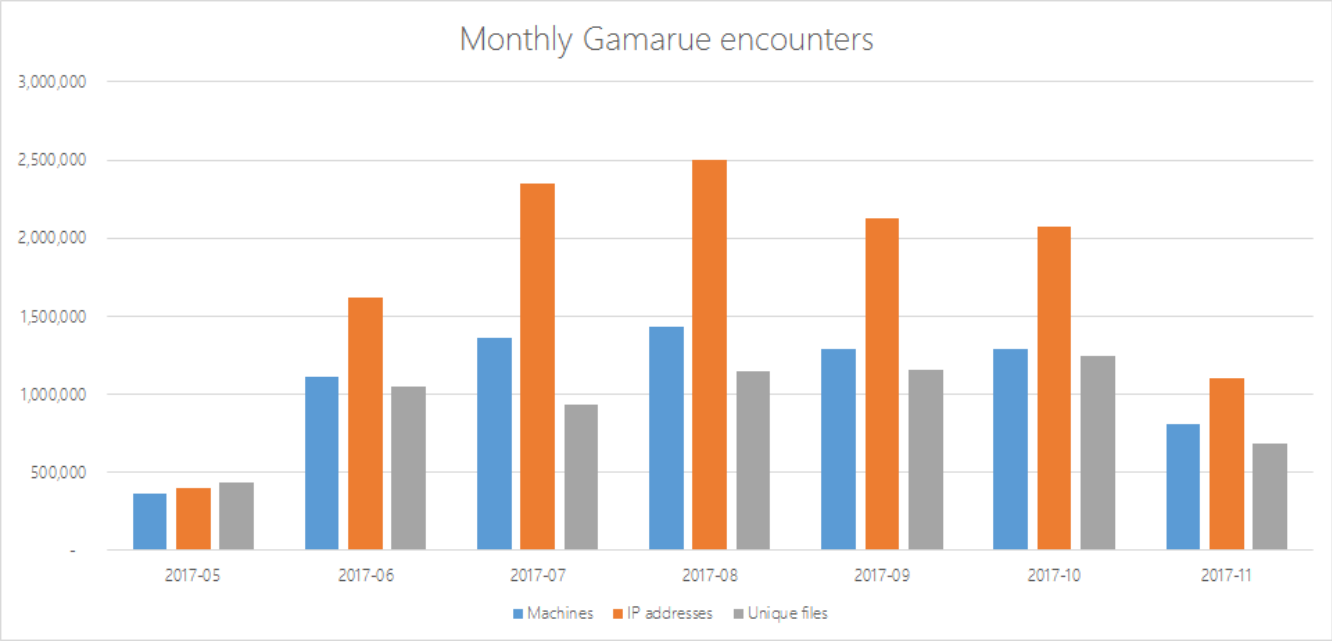

Figure 3. Machines, IPs, and unique file encounters for Gamarue from May to November 2017; data does not include LNK detections

The Gamarue bot

Gamarue is known in the underground cybercrime market as Andromeda bot. A bot is a program that allows an attacker to take control of an infected machine. Like many other bots, Gamarue is advertised as a crime kit that hackers can purchase.

The Gamarue crime kit includes the following components:

- **Bot-builder**, which builds the malware binary that infects computers
- **Command-and-control application**, which is a PHP-based dashboard application that allows hackers to manage and control the bots
- **Documentation** on how to create a Gamarue botnet

A botnet is a network of infected machines that communicate with command-and-control (C&C) servers, which are computer servers used by the hacker to control infected machines.

The evolution of the Gamarue bot has been the subject of many thorough analyses by security researchers. At the time of takedown, there were five known active Gamarue versions: 2.06, 2.07, 2.08, 2.09, and 2.10. The latest and the most active is version 2.10.

Gamarue is modular, which means that its functionality can be extended by plugins that are either included in the crime kit or available for separate purchase. The Gamarue plugins include:

- **Keylogger ($150)** – Used for logging keystrokes and mouse activity in order to steal user names and passwords, financial information, etc
- **Rootkit (included in crime kit)** – Injects rootkit codes into all processes running on a victim computer to give Gamarue persistence
- **Socks4/5 (included in crime kit)** – Turns victim computer into a proxy server for serving malware or malicious instructions to other computers on the internet
- **Formgrabber ($250)** – Captures any data submitted through web browsers (Chrome, Firefox, and Internet Explorer)

- **Teamviewer ($250)** – Enables attacker to remotely control the victim machine, spy on the desktop, perform file transfer, among other functions
- **Spreader** – Adds capability to spread Gamarue malware itself via removable drives (for example, portable hard drives or flash drives connected via a USB port); it also uses Domain Name Generation (DGA) for the servers where it downloads updates

Gamarue attack kill-chain

Over the years, various attack vectors have been used to distribute Gamarue. These include:

- Removable drives
- Social media (such as Facebook) messages with malicious links to websites that host Gamarue
- Drive-by downloads/exploit kits
- Spam emails with malicious links
- Trojan downloaders

Once Gamarue has infected a machine, it contacts the C&C server, making the machine part of the botnet. Through the C&C server, the hacker can control Gamarue-infected machines, steal information, or issue commands to download additional malware modules.

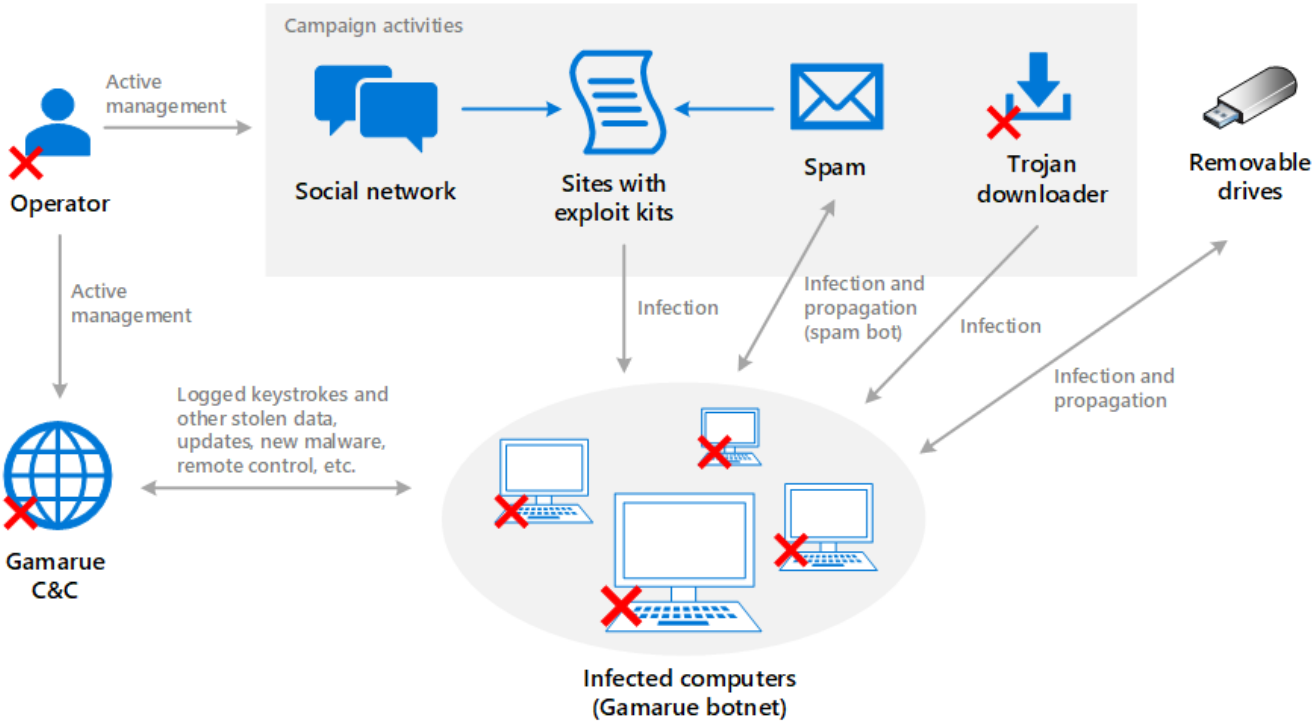

Figure 4. Gamarue's attack kill-chain

Gamarue's main goal is to distribute other prevalent malware families. During the CME campaign, we saw at least 80 different malware families distributed by Gamarue. Some of these malware families include:

- Petya (ransomware)
- Cerber (ransomware)
- Troldesh (ransomware)
- Ursnif (info-stealing and banking trojan)
- Carberp (info-stealing and banking trojan)
- Fareit (info-stealing and DDoS malware)
- Kasidet (worm and DDoS malware)

- Lethic (spam bot)
- Cutwail (spam bot)
- Neurevt (click-fraud malware)
- Ursnif (click-fraud malware)
- Fynloski (backdoor)

The installation of other malware broadens the scale of what hackers can do with the network of infected machines.

Command-and-control communication

When the Gamarue malware triggers the infected machine to contact the C&C server, it provides information like the hard disk's volume serial number (used as the bot ID for the computer), the Gamarue build ID, the operating system of the infected machine, the local IP address, an indication whether the signed in user has administrative rights, and keyboard language setting for the infected machine. This information is sent to the C&C server via HTTP using the JSON format:

```
{"id":%lu,"bid":%lu,"os":%lu,"la":%lu,"rg":%lu,"bb":%lu',0
```

Figure 5. Information sent by Gamarue to C&C server

The information about keyboard language setting is very interesting, because the machine will not be further infected if the keyboard language corresponds to the following countries:

- Belarus
- Russia
- Ukraine
- Kazahkstan

Before sending to the C&C server, this information is encrypted with RC4 algorithm using a key hardcoded in the Gamarue malware body.

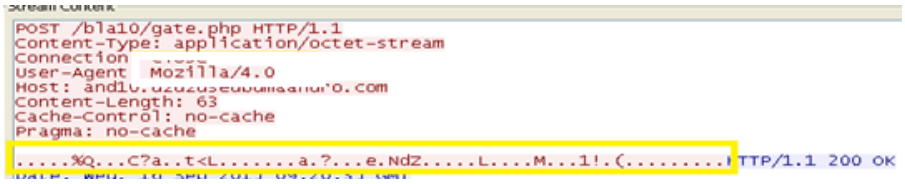

Figure 6. Encrypted C&C communication

Once the C&C server receives the message, it sends a command that is pre-assigned by the hacker in the control dashboard.

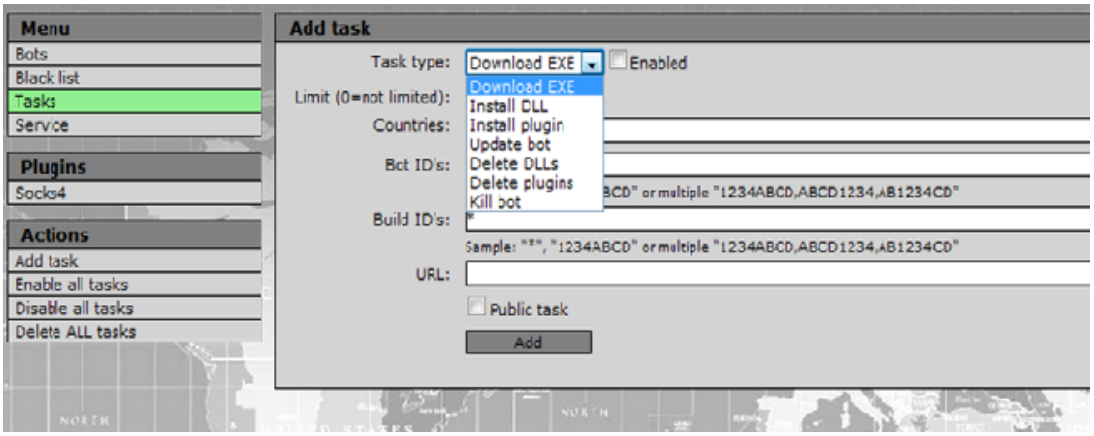

Figure 7. Sample control dashboard used by attackers to communicate to Gamarue bots

The command can be any of the following:

- Download EXE (i.e., additional executable malware files)
- Download DLL (i.e., additional malware; removed in version 2.09 and later)
- Install plugin
- Update bot (i.e., update the bot malware)
- Delete DLLs (removed in version 2.09 and later)
- Delete plugins
- Kill bot

The last three commands can be used to remove evidence of Gamarue presence in machines.

The reply from the C&C server is also encrypted with RC4 algorithm using the same key used to encrypt the message from the infected machine.

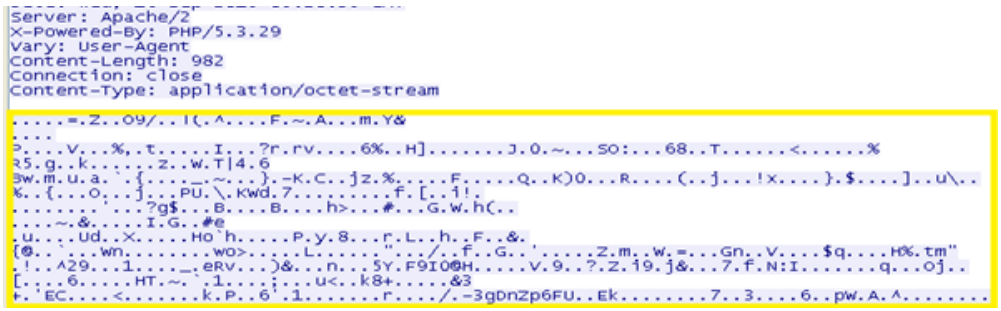

Figure 8. Encrypted reply from C&C server

When decrypted, the reply contains the following information:

- Time interval in minutes – time to wait for when to ask the C2 server for the next command
- Task ID – used by the hacker to track if there was an error performing the task
- Command – one of the command mentioned above
- Download URL – from which a plugin/updated binary/other malware can be downloaded depending on the command.

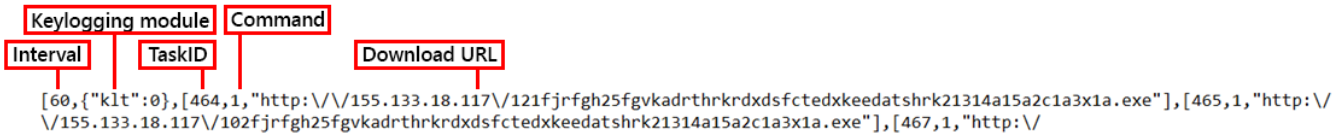

Figure 9. Decrypted reply from C&C server

Anti-sandbox techniques

Gamarue employs anti-AV techniques to make analysis and detection difficult. Prior to infecting a machine, Gamarue checks a list hashes of the processes running on a potential victim's machine. If it finds a process that may be associated with malware analysis tools, such as virtual machines or sandbox tools, Gamarue does not infect the machine. In older versions, a fake payload is manifested when running in a virtual machine.

```
analysis_prog_hash_list dd 99DD4432h    ; DATA XREF: chk_dbg+C8↓r
                                        ; chk_dbg+DD↓r
                                        ; vmwareuser.exe
                        dd 2D859DB4h    ; vmwareservice.exe
                        dd 64340DCEh    ; vboxservice.exe
                        dd 63C54474h    ; vboxtray.exe
                        dd 349C9C8Bh    ; sandboxiedcomlaunch.exe
                        dd 3446EBCEh    ; sandboxierpcss.exe
                        dd 5BA9B1FEh    ; procmon.exe
                        dd 3CE2BEF3h    ; regmon.exe
                        dd 3D46F02Bh    ; filemon.exe
                        dd 77AE10F7h    ; wireshark.exe
                        dd 0F344E95Dh   ; netmon.exe
```

Figure 10. Gamarue checks if any of the running processes are associated with malware analysis tools

Stealth mechanisms

Gamarue uses cross-process injection techniques to stay under the radar. It injects its code into the following legitimate processes:

- msiexec.exe (Gamarue versions 2.07 to 2.10)
- wuauclt.exe, wupgrade.exe, svchost.exe (version 2.06)

It can also use a rootkit plugin to hide the Gamarue file and its autostart registry entry.

Gamarue employs a stealthy technique to store and load its plugins as well. The plugins are stored fileless, either saved in the registry or in an alternate data stream of the Gamarue file.

OS tampering

Gamarue attempts to tamper with the operating systems of infected computers by disabling Firewall, Windows Update, and User Account Control functions. These functionalities cannot be re-enabled until the Gamarue infection has been removed from the infected machine. This OS tampering behavior does not work on Windows 10

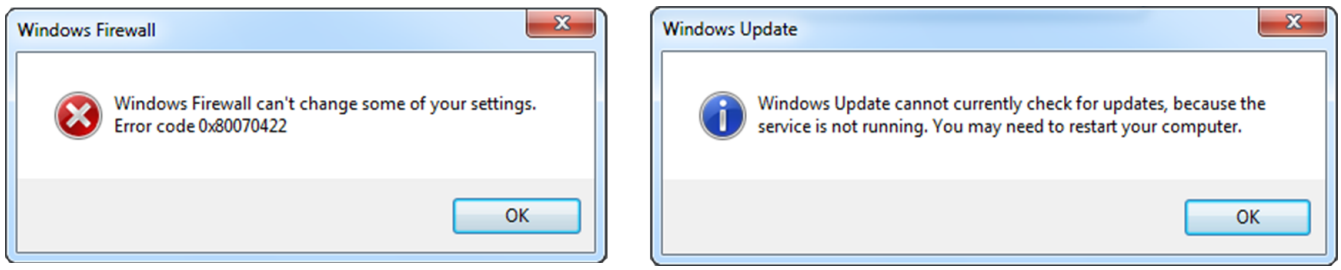

Figure 11. Disabled Firewall and Windows Update

Monetization

There are several ways hackers earn using Gamarue. Since Gamarue's main purpose is to distribute other malware, hackers earn using pay-per-install scheme. Using its plugins, Gamarue can also steal user information; stolen information can be sold to other hackers in cybercriminal underground markets. Access to Gamarue-infected machines can also be sold, rented, leased, or swapped by one criminal group to another.

Remediation

To help prevent a Gamarue infection, as well as other malware and unwanted software, take these precautions:

- Be cautious when opening emails or social media messages from unknown users.
- Be wary about downloading software from websites other than the program developers.

More importantly, ensure you have the right security solutions that can protect your machine from Gamarue and other threats. Windows Defender Antivirus detects and removes the Gamarue malware. With advanced machine learning models, as well as generic and heuristic techniques, Windows Defender AV detects new as well as never-before-seen malware in real-time via the cloud protection service. Alternatively, standalone tools, such as Microsoft Safety Scanner and the Malicious Software Removal Tool (MSRT), can also detect and remove Gamarue.

Microsoft Edge can block Gamarue infections from the web, such as those from malicious links in social media messages and drive-by downloads or exploit kits. Microsoft Edge is a secure browser that opens pages within low privilege app containers and uses reputation-based blocking of malicious downloads.

In enterprise environments, additional layers of protection are available. Windows Defender Advanced Threat Protection can help security operations personnel to detect Gamarue activities, including cross-process injection techniques, in the network so they can investigate and respond to attacks. Windows Defender ATP's enhanced behavioral and machine learning detection libraries flag malicious behavior across the malware infection process, from delivery and installation, to persistence mechanisms, and command-and-control communication.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Microsoft Exchange Online Protection (EOP) can block Gamarue infections from email uses built-in anti-spam filtering capabilities that help protect Office 365 customers. Office 365 Advanced Threat Protection helps secure mailboxes against email attacks by blocking emails with unsafe attachments, malicious links, and linked-to files leveraging time-of-click protection.

Windows Defender Exploit Guard can block malicious documents (such as those that distribute Gamarue) and scripts. The Attack Surface Reduction (ASR) feature in Windows Defender Exploit Guard uses a set of built-in intelligence that can block malicious behaviors observed in malicious documents. ASR rules can also be turned on to block malicious attachments from being run or launched from Microsoft Outlook or webmail (such as Gmail, Hotmail, or Yahoo).

Microsoft is also continuing the collaborative effort to help clean Gamarue-infected computers by providing a one-time package with samples (through the Virus Information Alliance) to help organizations protect their customers.

Microsoft Digital Crimes Unit** and **Windows Defender Research team

Get more info on the Gamarue (Andromeda) takedown from the following sources:

- Europol: Andromeda botnet dismantled in international cyber operation
- ESET: ESET unites with Microsoft and law enforcement agencies to disrupt Gamarue botnets

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.