Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

Ryan Sherstobitoff

Apr 24, 2018

17 MIN READ

McAfee Advanced Threat Research analysts have uncovered a global data reconnaissance campaign assaulting a wide number of industries including critical infrastructure, entertainment, finance, health care, and telecommunications. This campaign, dubbed Operation GhostSecret, leverages multiple implants, tools, and malware variants associated with the state-sponsored cyber group Hidden Cobra. The infrastructure currently remains active. In this post, we dive deeply into this campaign. For a brief overview of this threat, see “Global Malware Campaign Pilfers Data from Critical Infrastructure, Entertainment, Finance, Health Care, and Other Industries.”

Our investigation into this campaign reveals that the actor used multiple malware implants, including an unknown implant with capabilities similar to Bankshot. From March 18 to 26 we observed the malware operating in multiple areas of the world. This new variant resembles parts of the Destover malware, which was used in the 2014 Sony Pictures attack.

Furthermore, the Advanced Threat Research team has discovered Proxysvc, which appears to be an undocumented implant. We have also uncovered additional control servers that are still active and associated with these new implants. Based on our analysis of public and private information from submissions, along with product telemetry, it appears Proxysvc was used alongside the 2017 Destover variant and has operated undetected since mid-2017.

The attackers behind Operation GhostSecret used a similar infrastructure to earlier threats, including SSL certificates used by FakeTLS in implants found in the Destover backdoor variant known as Escad, which was used in the Sony Pictures attack. Based on our technical analysis, telemetry, and data from submissions, we can assert with high confidence that this is the work of the Hidden Cobra group. The Advanced Threat Research team uncovered activity related to this campaign in March 2018, when the actors targeted Turkish banks. These initial findings appear to be the first stage of Operation GhostSecret. For more on the global aspect of this threat, see “Global Malware Campaign Pilfers Data from Critical Infrastructure of Entertainment, Finance, Health Care, and Other Industries.”

Analysis

The McAfee Advanced Threat Research team discovered a previously unknown data-gathering implant that surfaced in mid-February 2018. This implant appears to be a derivative of implants authored before by Hidden Cobra and contains functionality similar to that of Bankshot, with code overlaps from other Hidden Cobra implants. However, the variant is not based on Bankshot. Our analysis of the portable executable’s rich-header data reveals that the two implants were compiled in different development environments. (The PE rich header is an undocumented part of a Windows executable that reveals unique information to identify the Microsoft compiler and linker used to create the program. It is helpful for identifying similarities between malware variants to establish common development environments.) Our analysis of the code and PE rich header indicates that Bankshot, Proxysvc, and the Destover-like implant are distinct families, but also contain overlapping code and functionality with current tools of Hidden Cobra.

PE rich header data from the 2018 Bankshot implant.

PE rich header data from the new February 2018 implant.

PE rich header data from Proxysvc.dll.

When we compared the PE rich header data of the new February 2018 implant with a variant of Backdoor.Escad (Destover) from 2014 shortly before the Sony Pictures attack, we found the signatures to be identical. The Destover-like variant is 83% similar in code to a 2015 variant and contains the same rich PE header signature as the Backdoor.Escad variant we analyzed. Thus the new implant is likely a derivative of components of Destover. We determined that the implant is not a direct copy of well-known previous samples of Destover; rather, Hidden Cobra created a new hybrid variant using functionality present in earlier versions.

2014 Backdoor.Escad (hash: 8a7621dba2e88e32c02fe0889d2796a0c7cb5144).

2015 Destover variant (7fe373376e0357624a1d21cd803ce62aa86738b6).

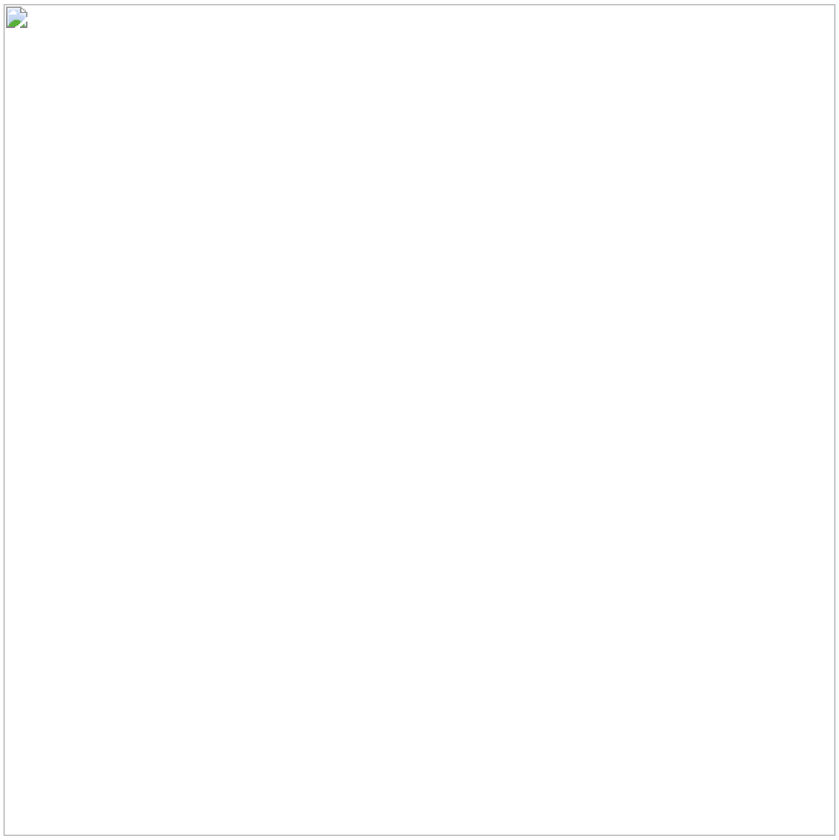
The February implant fe887fcab66d7d7f79f05e0266c0649f0114ba7c was obtained from an unknown submitter in the United States on February 14, two days after it was compiled. This Korean-language file used the control server IP address 203.131.222.83. The implant is nearly identical to an unknown 2017 sample (8f2918c721511536d8c72144eabaf685ddc21a35) except that the control server addresses are different. The 2017 sample used address 14.140.116.172. Both implants specifically use FakeTLS with PolarSSL, which we saw in previous Hidden Cobra implants. PolarSSL libraries have appeared in implants since the Sony Pictures incident and were used exclusively in the implant Backdoor.Destover. This implant incorporated a custom control server protocol that sends traffic over port 443. The implementation does not format the packets in standard SSL, but rather in a custom format and transmitted over SSL—hence, FakeTLS. The control server traffic when compared to Backdoor.Escad is nearly identical.

TLS traffic in Backdoor.Destover, the 2018 Destover-like variant.

TLS traffic in Backdoor.Escad.

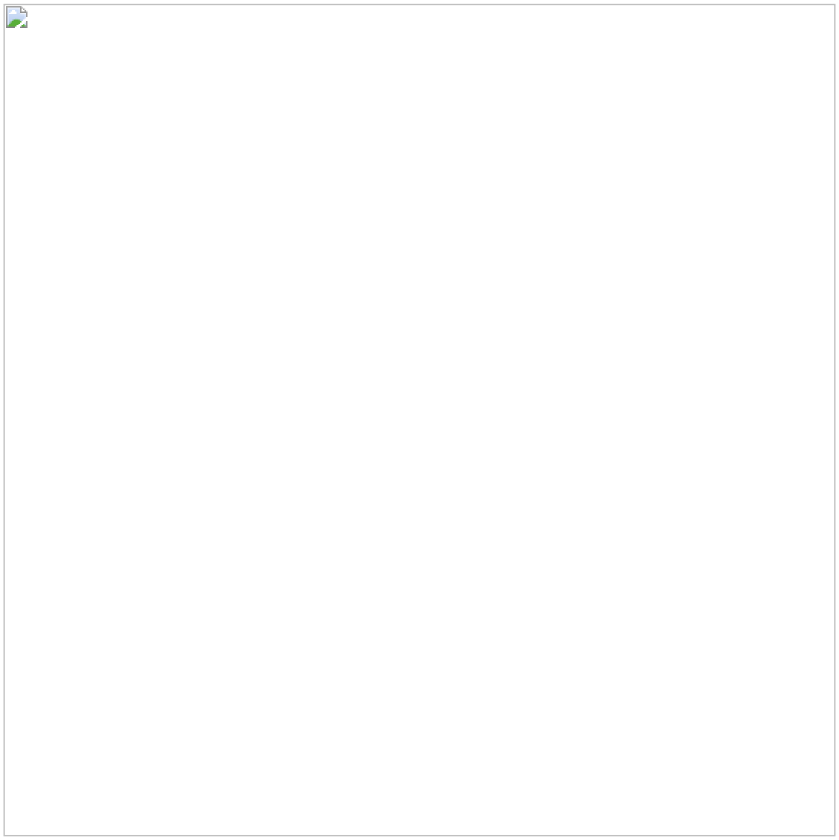
Further research into IP address 14.140.116.172 leads us to additional hidden components involved in the overall infrastructure. Proxysvc.dll contains a list of hardcoded IP addresses, including the preceding address, all located in India. Despite the name, this component is not an SSL proxy, but rather a unique data-gathering and implant-installation component that listens on port 443 for inbound control server connections.

Proxysvc was first collected by public and private sources on March 22 from an unknown entity in the United States. The executable dropper for the component was submitted from South Korea on March 19. McAfee telemetry analysis from March 16 to 21 reveals that Proxysvc components were active in the wild. Our research shows this listener component appeared mostly in higher education organizations. We suspect this component is involved in core control server infrastructure. These targets were chosen intentionally to run Proxysvc because the attacker would have needed to know which systems were infected to connect to them. This data also indicates this infrastructure had been operating for more than a year before its discovery. The Advanced Threat Research team found this component running on systems in 11 countries. Given the limited capabilities of Proxysvc, it appears to be part of a covert network of SSL listeners that allow the attackers to gather data and install more complex implants or additional infrastructure. The SSL listener supports multiple control server connections, rather than a list of hardcoded addresses. By removing the dependency on hardcoded IP addresses and accepting only inbound connections, the control service can remain unknown.



The number of infected systems by country in which Proxysvc.dll was operating in March. Source: McAfee Advanced Threat Research.

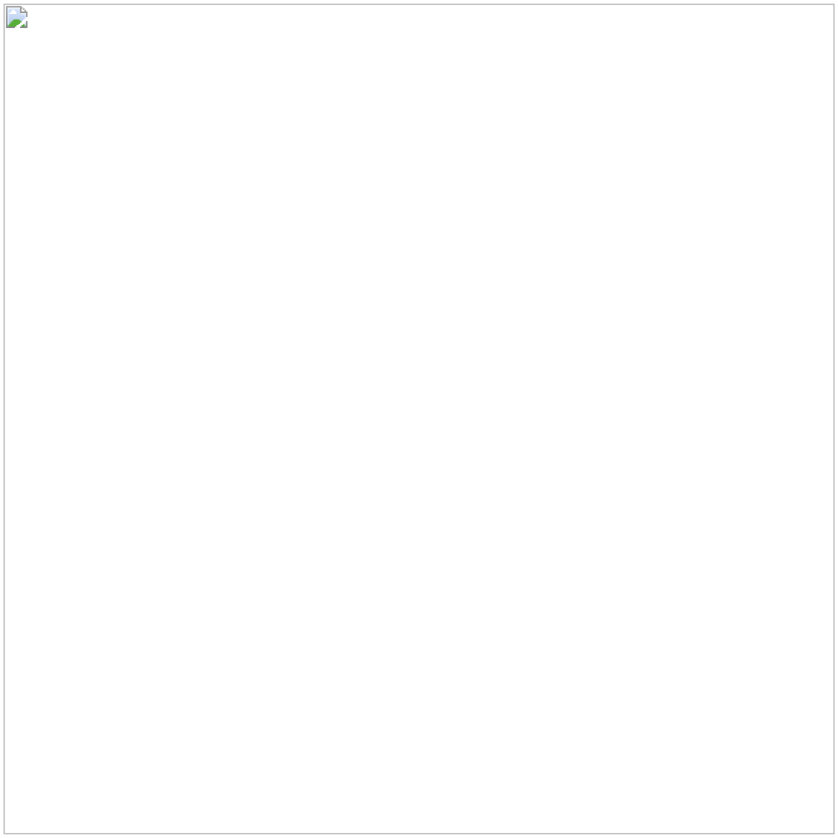
The 2018 Destover-like implant appeared in organizations in 17 countries between March 14 and March 18. The impacted organizations are in industries such as telecommunications, health, finance, critical infrastructure, and entertainment.

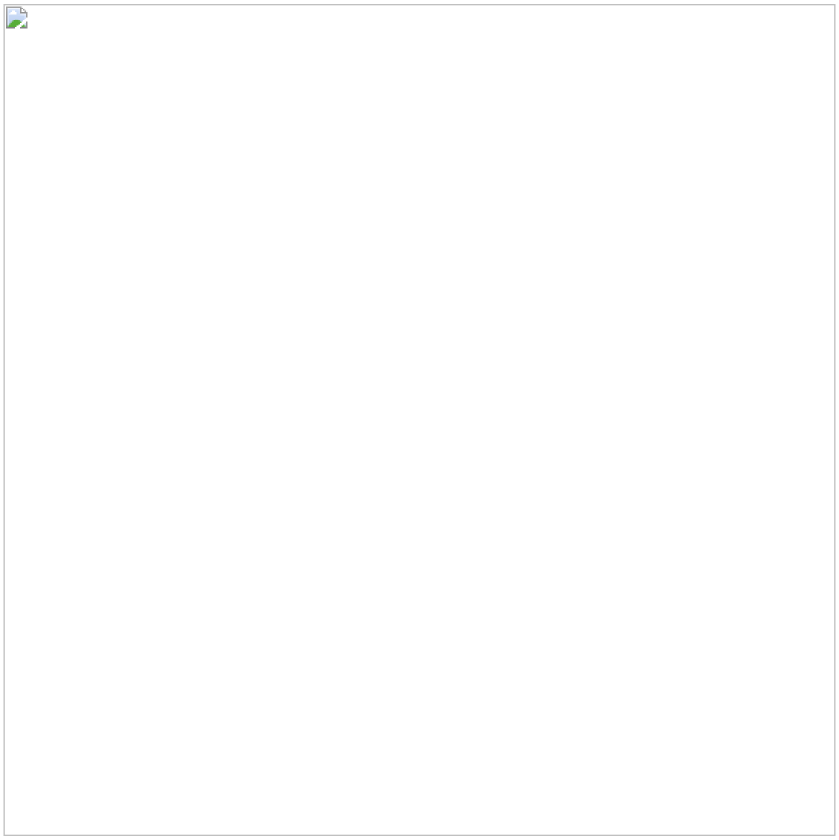


The number of infected systems by country in which the Destover variant was operating in March. Source: McAfee Advanced Threat Research.

Control Servers

Further investigation into the control server infrastructure reveals the SSL certificate d0cb9b2d4809575e1bc1f4657e0eb56f307c7a76, which is tied to the control server 203.131.222.83, used by the February 2018 implant. This server resides at Thammasat University in Bangkok, Thailand. The same entity hosted the control server for the Sony Pictures implants. This SSL certificate has been used in Hidden Cobra operations since the Sony Pictures attack. Analyzing this certificate reveals additional control servers using the same PolarSSL certificate. Further analysis of McAfee telemetry data reveals several IP addresses that are active, two within the same network block as the 2018 Destover-like implant.





Number of infections by Thammasat University–hosted control servers from March 15–19, 2018. Source: McAfee Advanced Threat Research.

Implant Origins

McAfee Advanced Threat Research determined that the Destover-like variant originated from code developed in 2015. The code reappeared in variants surfacing in 2017 and 2018 using nearly the same functionality and with some modifications to commands, along with an identical development environment based on the rich PE header information.

Both implants (fe887fcab66d7d7f79f05e0266c0649f0114ba7c and 8f2918c721511536d8c72144eabaf685ddc21a35) are based on the 2015 code. When comparing the implant 7fe373376e0357624a1d21cd803ce62aa86738b6, compiled on August 8, 2015, we found it 83% similar to the implant from 2018. The key similarities and differences follow.

Similarities

- Both variants build their API imports dynamically using GetProcAddress, including wtsapi32.dll for gathering user and domain names for any active remote sessions
- Both variants contain a variety of functionalities based on command IDs issued by the control servers
- Common capabilities of both malware:
    - Listing files in directory
    - Creating arbitrary processes
    - Writing data received from control servers to files on disk
    - Gathering information for all drives
    - Gathering process times for all processes
    - Sending the contents of a specific file to the control server
    - Wiping and deleting files on disk
    - Setting the current working directory for the implant
    - Sending disk space information to the control server
- Both variants use a batch file mechanism to delete their binaries from the system
- Both variants run commands on the system, log output to a temporary file, and send the contents of the file to their control servers

Differences

The following capabilities in the 2015 implant are missing from the 2018 variant:

- Creating a process as a specific user
- Terminating a specific process

- Deleting a specific file
- Setting file times for a specific file
- Getting current system time and sending it to the control server
- Reading the contents of a file on disk. If the filepath specified is a directory, then listing the directory’s contents.
- Setting attributes on files

The 2015 implant does not contain a hardcoded value of the IP address it must connect to. Instead it contains a hardcoded sockaddr_in data structure (positioned at 0x270 bytes before the end of the binary) used by the connect() API to specify port 443 and control server IP addresses:

- 193.248.247.59
- 196.4.67.45

Both of these control servers used the PolarSSL certificate d0cb9b2d4809575e1bc1f4657e0eb56f307c7a76.

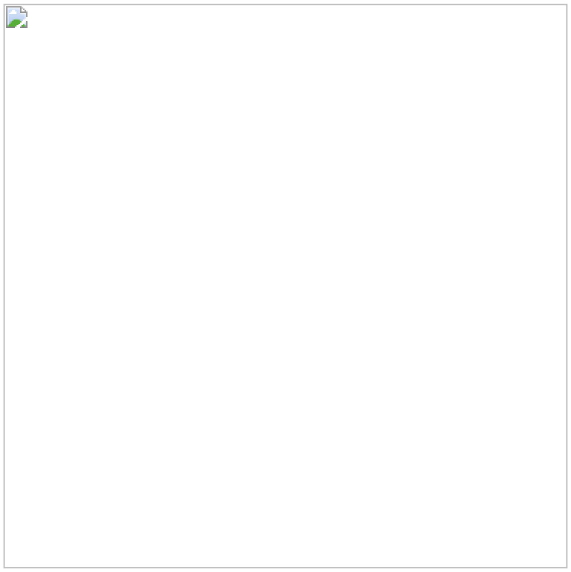
Proxysvc

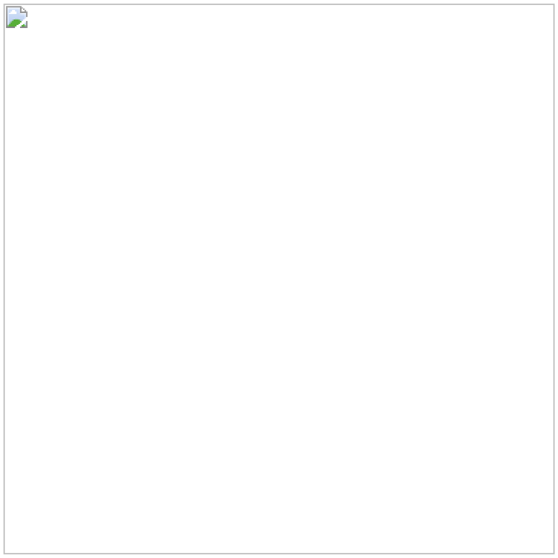
At first glance Proxysvc, the SSL listener, looks like a proxy setup tool (to carry out man-in-the-middle traffic interception). However, a closer analysis of the sample reveals it is yet another implant using HTTP over SSL to receive commands from the control server.

Proxysvc appears to be a downloader whose primary capability is to deliver additional payloads to the endpoint without divulging the control address of the attackers. This implant contains a limited set of capabilities for reconnaissance and subsequent payload installations. This implant is a service DLL that can also run as a standalone process.

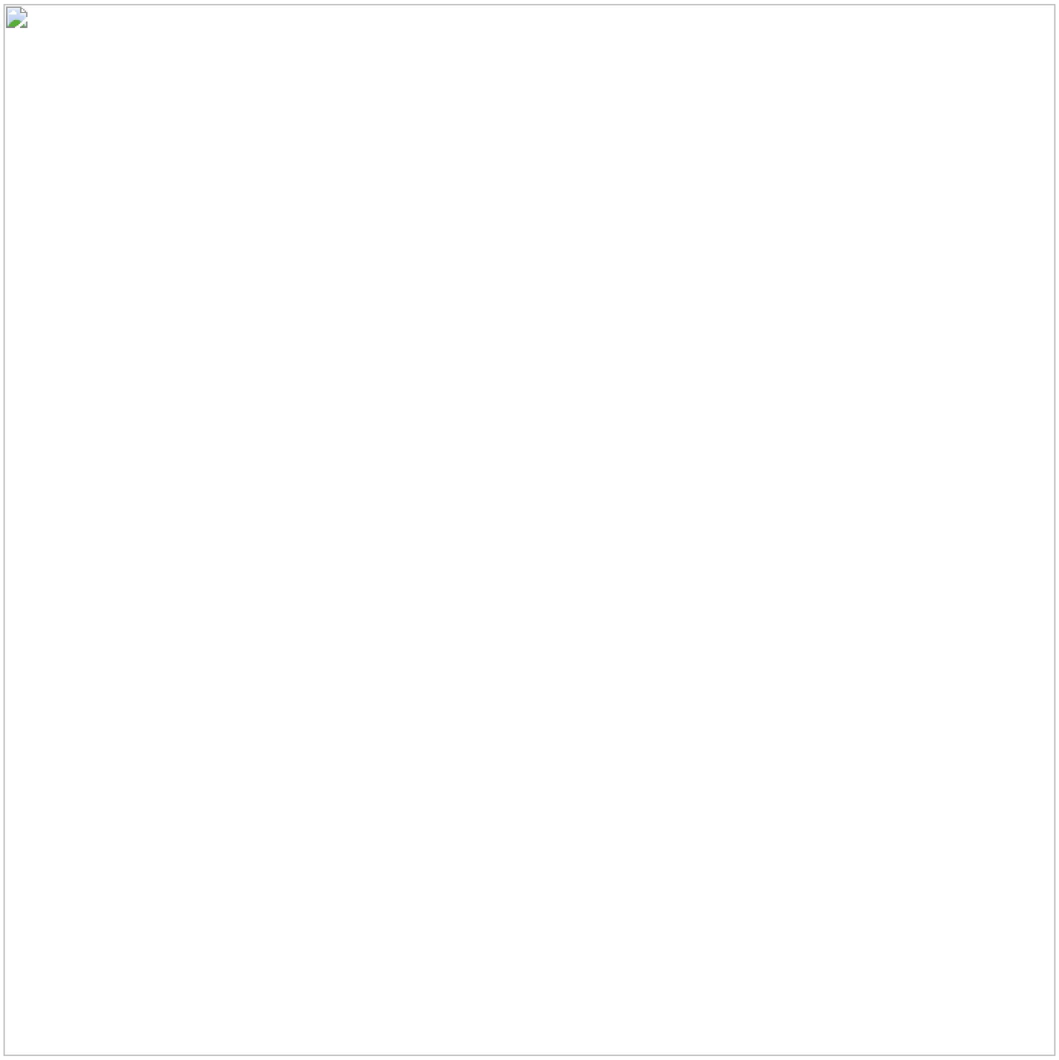
The ServiceMain() sub function of Proxysvc.

The implant cannot connect to a control server IP address or URL. Instead it accepts commands from the control server. The implant binds and listens to port 443 for any incoming connections.





Proxysvc binding itself to the specified port.



Proxysvc begins accepting incoming requests to process.

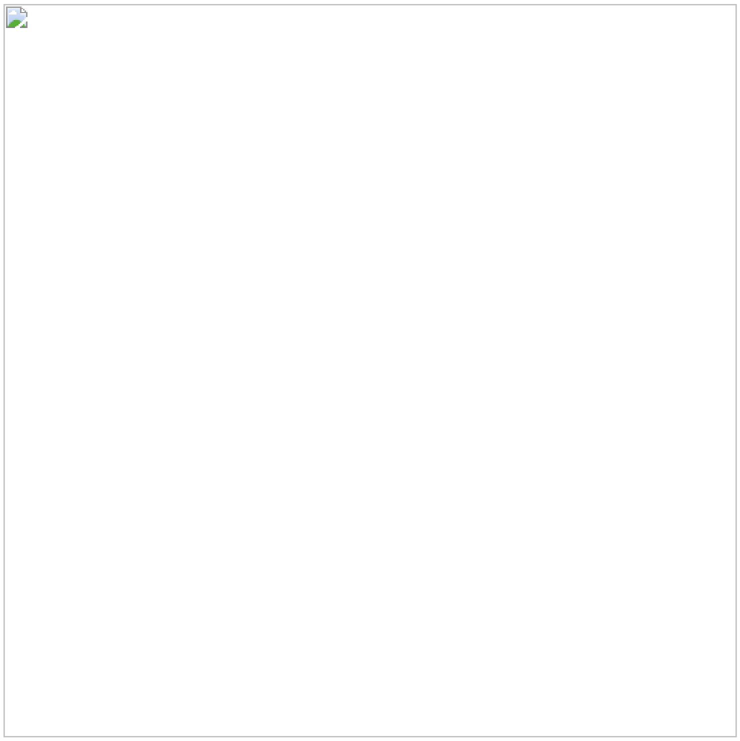
Proxysvc makes an interesting check while accepting connections from a potential control server. It checks against a list of IP addresses to make sure the incoming connection is *not* from any of the following addresses. If the incoming request does come from one of these, the implant offers a zero response (ASCII “0”) and shuts down the connection.

- 121.240.155.74
- 121.240.155.76
- 121.240.155.77
- 121.240.155.78
- 223.30.98.169
- 223.30.98.170
- 14.140.116.172

SSL Listener Capabilities

The implant receives HTTP-based commands from a control server and parses the HTTP Content-Type and Content-Length from the HTTP header. If the HTTP Content-Type matches the following value, then the implant executes the command specified by the control server:

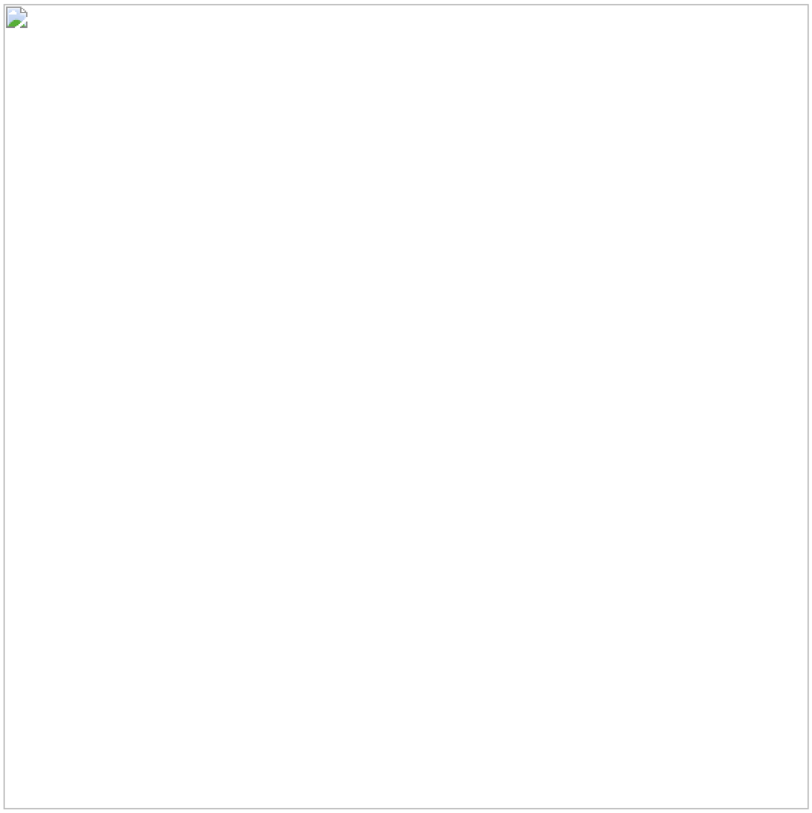
Content-Type: 8U7y3Ju387mVp49A



HTTP Content-Type comparison with a custom implant value.

The implant has the following capabilities:

- Writing an executable received from the control server into a temp file and executing it



Proxysvc writing a binary to a temp directory and executing it.

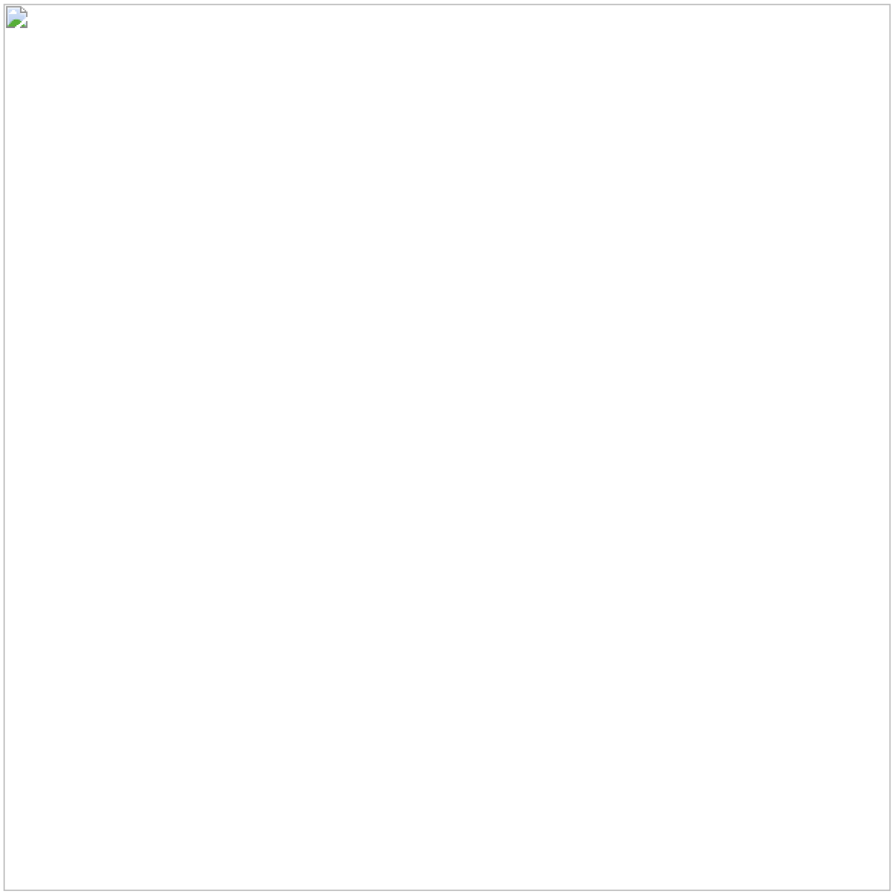
- Gathering system information and sending it to the control server. The system information gathered from the endpoint includes:
    - MAC address of the endpoint
    - Computer Name
    - Product name from HKLM\Software\Microsoft\Windows NT\CurrentVersion ProductName
    - This information is concatenated into a single string in the format: “MAC_Address|ComputerName|ProductName” and is sent to the control server
- Recording HTTP requests from the control server to the temporary file prx in the implant’s install directory with the current system timestamp

Analyzing the Main Implant

The February 2018 implant contains a wide variety of capabilities including data exfiltration and arbitrary command execution on the victim’s system. Given the extensive command structure that the implant can receive from the control server, this is an extensive framework for data reconnaissance and exfiltration, and indicates advanced use. For example, the implant can wipe and delete files, execute additional implants, read data out of files, etc.

The implant begins execution by dynamically loading APIs to perform malicious activities. Libraries used to load the APIs include:

- Kernel32.dll
- Apvapi32.dll
- Oleaut32.dll
- Iphlpapi.dll
- Ws2_32.dll
- Wtsapi32.dll
- Userenv.dll
- Ntdll.dll



The main implant dynamically loading APIs.

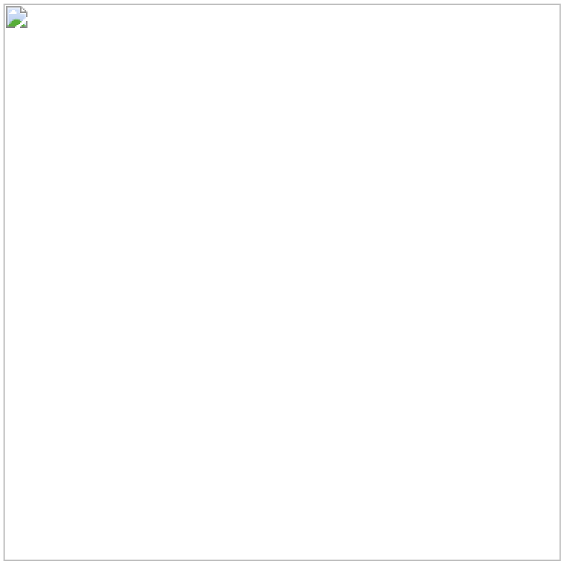
As part of its initialization, the implant gathers basic system information and sends it to its hardcoded control server 203.131.222.83 using SSL over port 443:

- Country name from system’s locale
- Operating system version

- Processor description from

HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 ProcessorNameString

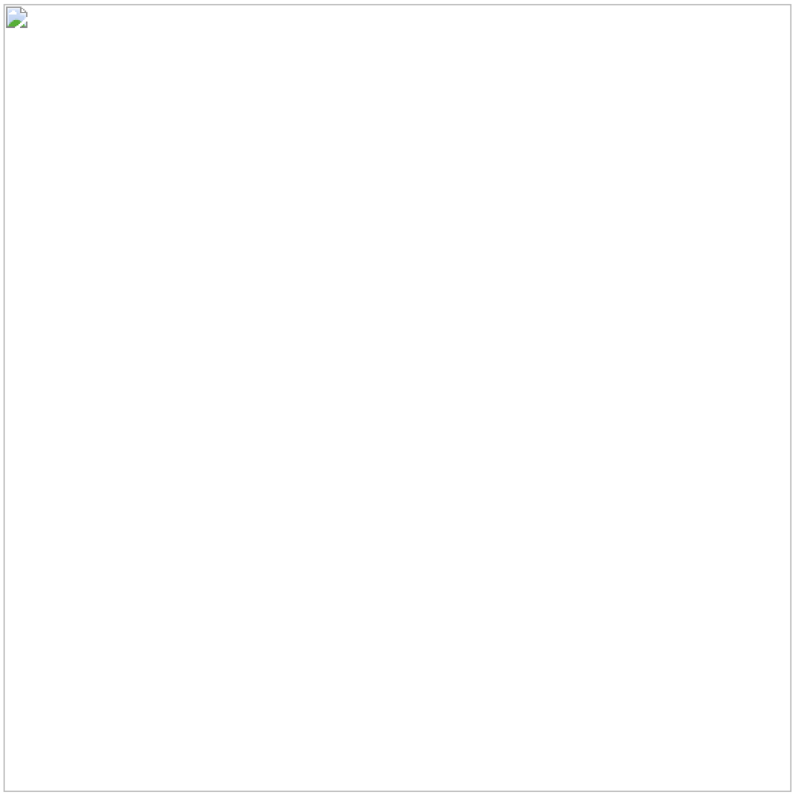
- Computer name and network adapters information
- Disk space information for disks C: through Z: including total memory in bytes, total available memory in bytes, etc.
- Current memory status including total physical memory in bytes, total available memory, etc.
- Domain name and usernames based on current remote sessions



Domain name and username extraction using Win32 WTS APIs.

Data Reconnaissance

The implant receives commands over SSL as encoded data. This data is decoded, and the correct command ID is derived. Valid command IDs reside between 0 and 0x1D.



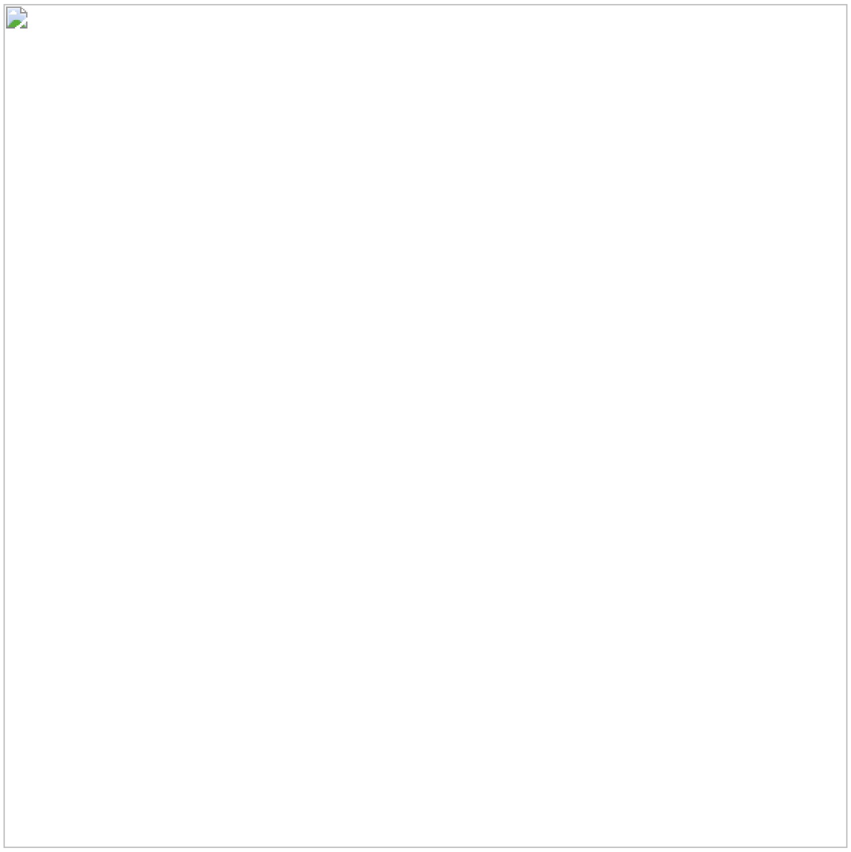
Switch case handling command execution based on command IDs.

Based on the command ID, the implant can perform the following functions:

- Gather system information and exfiltrate to the control server (same as the basic data-gathering functionality previously described)
- Get volume information for all drives on the system (A: through Z:) and exfiltrate to the control server

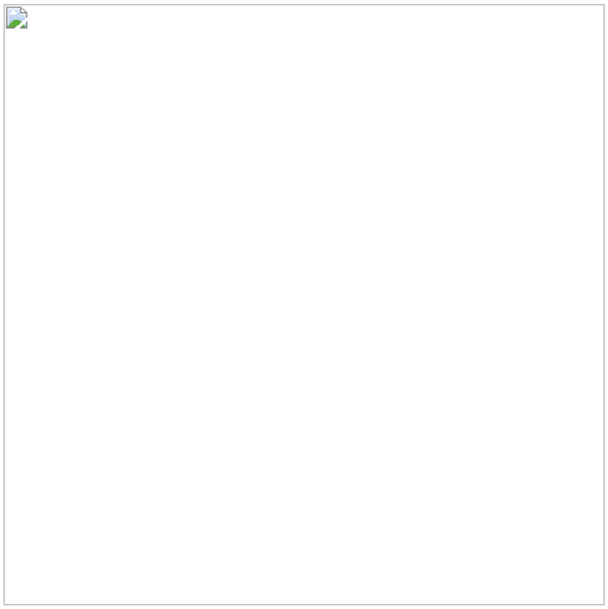
Gathering volume information.

- List files in a directory. The directory path is specified by the control server.
- Read the contents of a file and send it to the control server

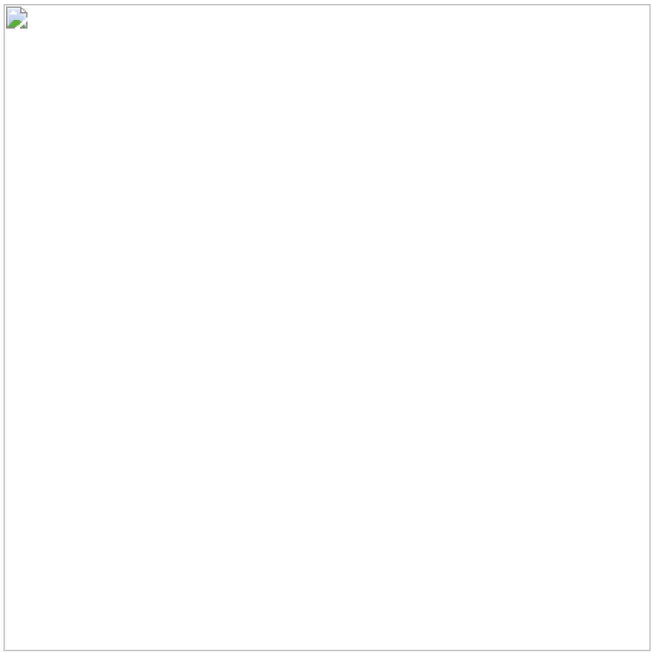


Reading file contents and sending it the control server.

Write data sent by the control server to a specified file path

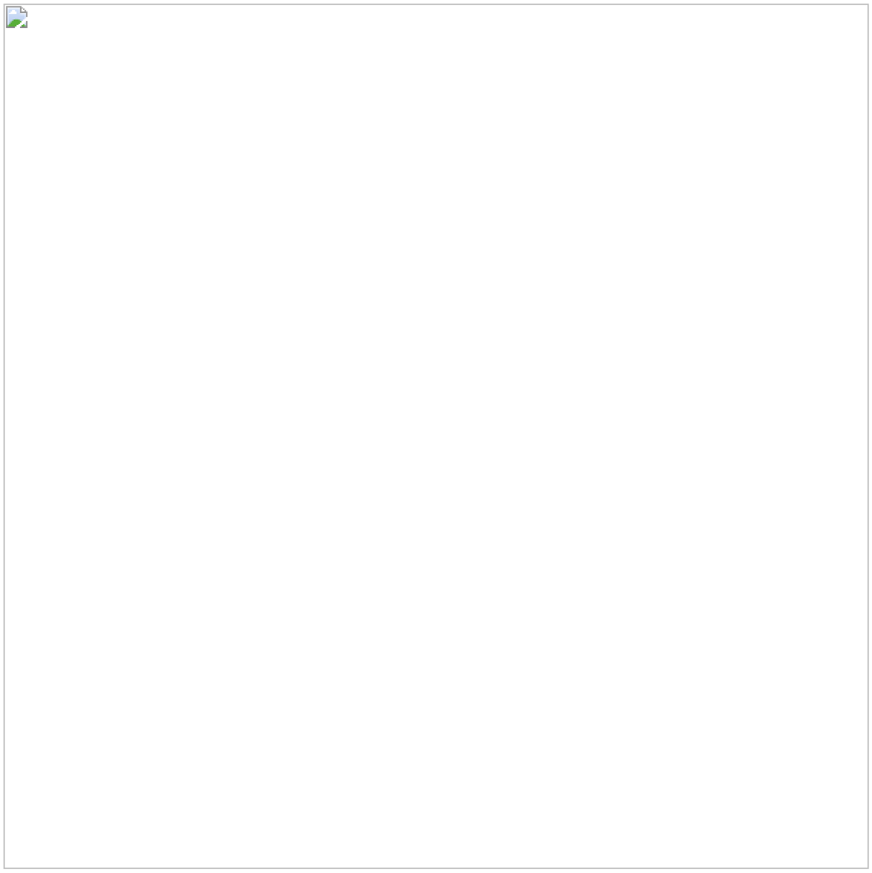


Open handle to a file for writing with no shared permissions.



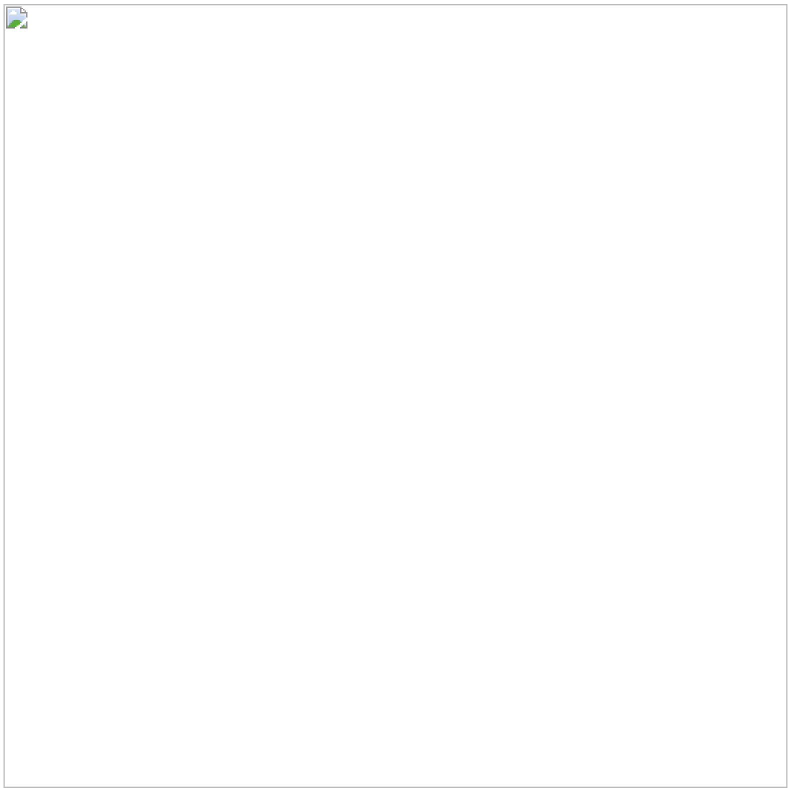
Writing data received from control server to file.

Create new processes based on the file path specified by the control server.



Creating a new process for a binary specified by the control server.

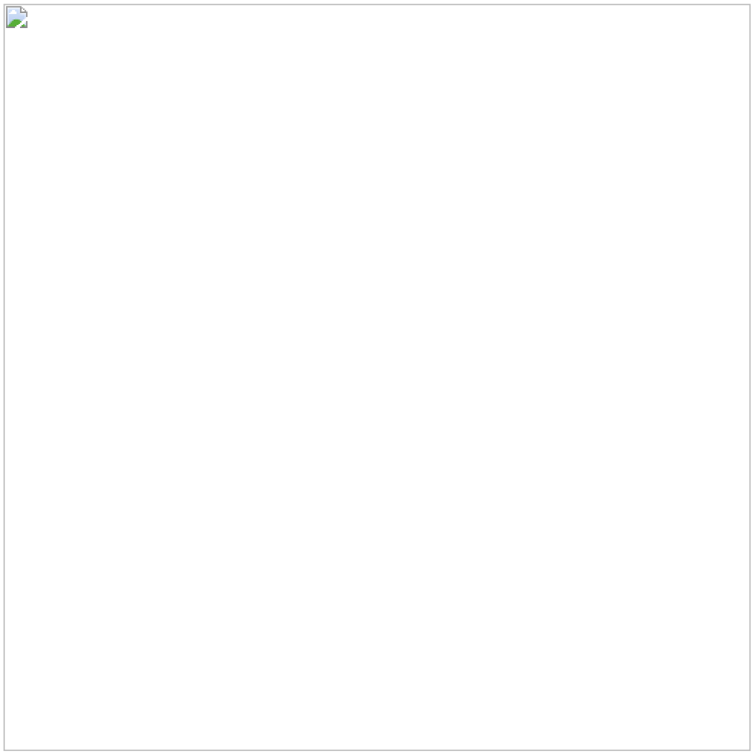
Wipe and delete files specified by the control server



Wiping and deleting files.

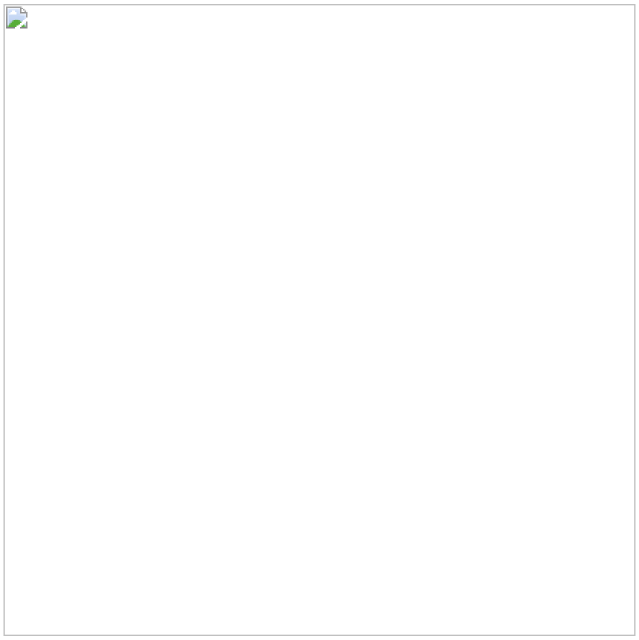
Execute a binary on the system using cmd.exe and log the results into a temp file, which is then read and the logged results are sent to the control server. The command line:

cmd.exe /c “<file_path> > %temp%\PM*.tmp 2>&1”

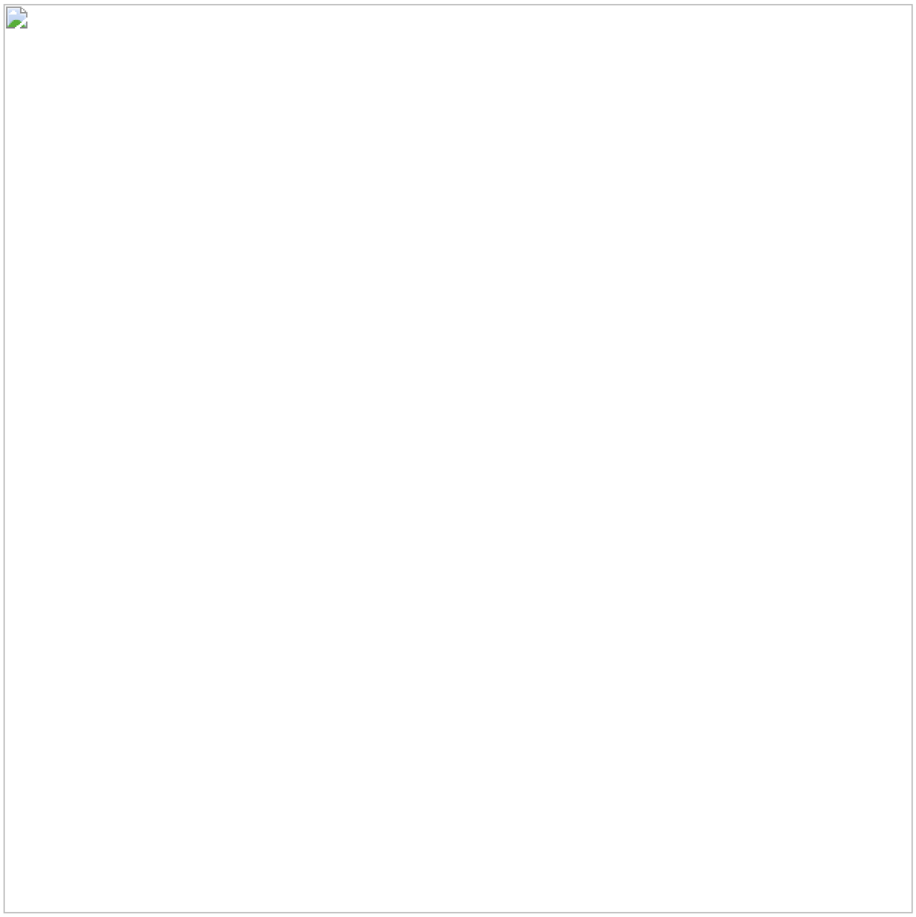


Executing a command and logging results to a temp file.

Get information for all currently running processes

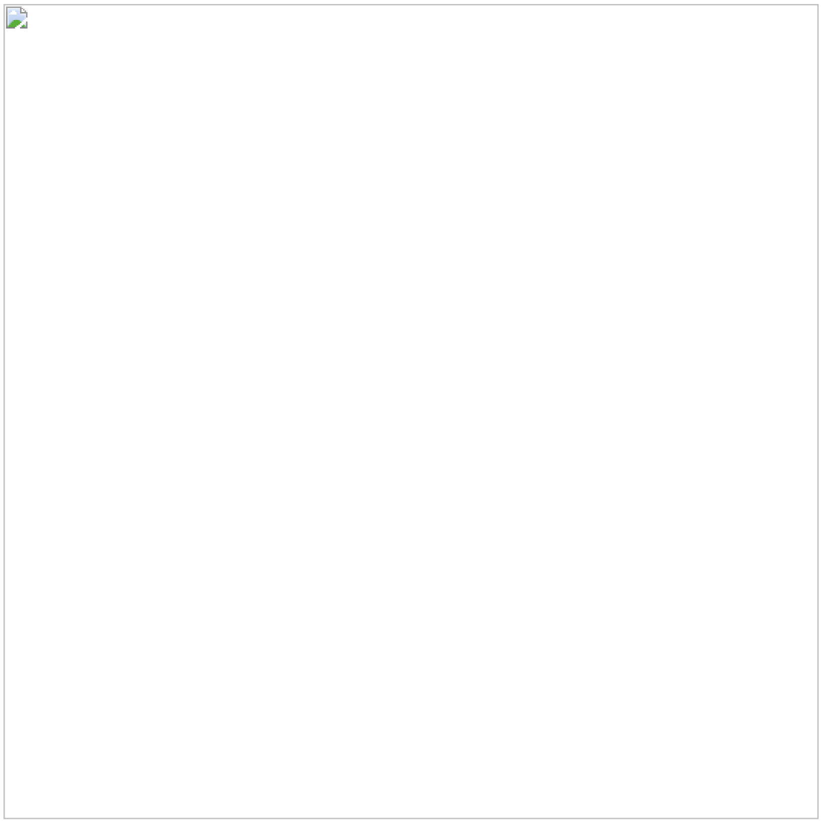


Getting process times for all processes on the system.



Getting username and domain from accounts associated with a running process.

Delete itself from disk using a batch file.

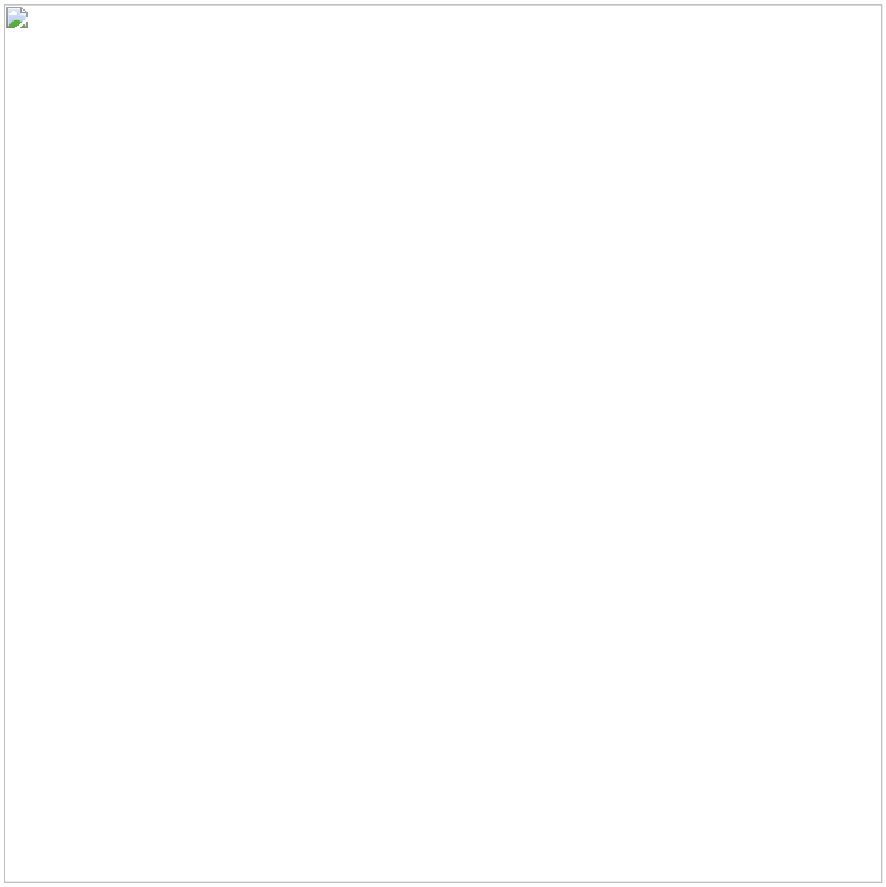


Creating a batch file for self-deletion.

Store encoded data received from the control server as a registry value at:

HKLM\Software\Microsoft\Windows\CurrentVersion\TowConfigs Description

Set and get the current working directory for the implant



Setting and getting the current working directory for the implant's process.

The command handler index table is organized in the implant as follows:

The command handler index table.

Conclusion

This analysis by the McAfee Advanced Threat Research team has found previously undiscovered components that we attribute to Hidden Cobra, which continues to target organizations around the world. The evolution in complexity of these data-gathering implants reveals an advanced capability by an attacker that continues its development of tools. Our investigation uncovered an unknown infrastructure connected to recent operations with servers in India using an advanced implant to establish a covert network to gather data and launch further attacks.

The McAfee Advanced Threat Research team will provide further updates as our investigation develops.

Fighting cybercrime is a global effort best undertaken through effective partnerships between the public and private sectors. McAfee is working with Thai government authorities to take down the control server infrastructure of Operation GhostSecret, while preserving the systems involved for further analysis by law enforcement authorities. By creating and maintaining partnerships with worldwide law enforcement, McAfee demonstrates that we are stronger together.

Indicators of Compromise

McAfee detection

Trojan-Bankshot2

MITRE ATT&CK techniques

- Exfiltration over control server channel: data is exfiltrated over the control server channel using a custom protocol
- Commonly used port: the attackers used common ports such as port 443 for control server communications
- Service execution: registers the implant as a service on the victim’s machine
- Automated collection: the implant automatically collects data about the victim and sends it to the control server

- Data from local system: local system is discovered and data is gathered
- Process discovery: implants can list processes running on the system
- System time discovery: part of the data reconnaissance method, the system time is also sent to the control server
- File deletion:: malware can wipe files indicated by the attacker

IP addresses

- 203.131.222.83
- 14.140.116.172
- 203.131.222.109

Hashes

- fe887fcab66d7d7f79f05e0266c0649f0114ba7c
- 8f2918c721511536d8c72144eabaf685ddc21a35
- 33ffbc8d6850794fa3b7bccb7b1aa1289e6eaa45

Ryan Sherstobitoff
Ryan Sherstobitoff is a Senior Analyst for Major Campaigns – Advanced Threat Research in McAfee. Ryan specializes in threat intelligence in the Asia Pacific Region where he conducts cutting edge...

More from McAfee Labs

Back to top