Symantec

SECURITY RESPONSE

Regin: Top-tier espionage tool enables stealthy surveillance

Symantec Security Response

Version 1.0 – November 24, 2014

“Regin is an extremely complex piece of software that can be customized with a wide range of different capabilities that can be deployed depending on the target.”

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

Symantec

CONTENTS

OVERVIEW 3
Introduction 5
Timeline 5
Target profile 6
  Infection vector 6
Architecture 8
  Stage 0 (dropper) 9
  Stage 1 9
  Stage 2 9
  Stage 3 9
  Stage 4 11
  Stage 5 11
  Encrypted virtual file system containers 11
  Command-and-control operations 12
  Logging 12
Payloads 14
64-bit version 15
  File names 15
  Stage differences 15
Conclusion 16
Protection 16
Appendix 18
  Data files 18
Indicators of compromise 20
  File MD5s 20
  File names/paths 20
  Extended attributes 21
  Registry 21

Symantec

OVERVIEW

In the world of malware threats, only a few rare examples can truly be considered groundbreaking and almost peerless. What we have seen in Regin is just such a class of malware.

Regin is an extremely complex piece of software that can be customized with a wide range of different capabilities which can be deployed depending on the target. It is built on a framework that is designed to sustain long-term intelligence-gathering operations by remaining under the radar. It goes to extraordinary lengths to conceal itself and its activities on compromised computers. Its stealth combines many of the most advanced techniques that we have ever seen in use.

The main purpose of Regin is intelligence gathering and it has been implicated in data collection operations against government organizations, infrastructure operators, businesses, academics, and private individuals. The level of sophistication and complexity of Regin suggests that the development of this threat could have taken well-resourced teams of developers many months or years to develop and maintain.

Regin is a multi-staged, modular threat, meaning that it has a number of components, each depending on others, to perform attack operations. This modular approach gives flexibility to the threat operators as they can load custom features tailored to individual targets when required. Some custom payloads are very advanced and exhibit a high degree of expertise in specialist sectors. The modular design also makes analysis of the threat difficult, as all components must be available in order to fully understand it. This modular approach has been seen in other sophisticated malware families such as Flamer and Weevil (The Mask), while the multi-stage loading architecture is similar to that seen in the Dugu/Stuxnet family of threats.

Regin is different to what are commonly referred to as “traditional” advanced persistent threats (APTs), both in its techniques and ultimate purpose. APTs typically seek specific information, usually intellectual property. Regin’s purpose is different. It is used for the collection of data and continuous monitoring of targeted organizations or individuals. This report provides a technical analysis of Regin based on a number of identified samples and components. This analysis illustrates Regin’s architecture and the many payloads at its disposal.

Symantec

INTRODUCTION

> “Regin has a wide range of standard capabilities, particularly around monitoring targets and stealing data.”

Introduction

Regin is a multi-purpose data collection tool which dates back several years. Symantec first began looking into this threat in the fall of 2013. Multiple versions of Regin were found in the wild, targeting several corporations, institutions, academics, and individuals.

Regin has a wide range of standard capabilities, particularly around monitoring targets and stealing data. It also has the ability to load custom features tailored to individual targets. Some of Regin's custom payloads point to a high level of specialist knowledge in particular sectors, such as telecoms infrastructure software, on the part of the developers.

Regin is capable of installing a large number of additional payloads, some highly customized for the targeted computer. The threat's standard capabilities include several remote access Trojan (RAT) features, such as capturing screenshots and taking control of the mouse's point-and-click functions. Regin is also configured to steal passwords, monitor network traffic, and gather information on processes and memory utilization. It can also scan for deleted files on an infected computer and retrieve them. More advanced payload modules designed with specific goals in mind were also found in our investigations. For example, one module was designed to monitor network traffic to Microsoft Internet Information Services (IIS) web servers, another was designed to collect administration traffic for mobile telephony base station controllers, while another was created specifically for parsing mail from Exchange databases.

Regin goes to some lengths to hide the data it is stealing. Valuable target data is often not written to disk. In some cases, Symantec was only able to retrieve the threat samples but not the files containing stolen data.

Timeline

Symantec is aware of two distinct versions of Regin. Version 1.0 appears to have been used from at least 2008 to 2011. Version 2.0 has been used from 2013 onwards, though it may have possibly been used earlier.

Version 1.0 appears to have been abruptly withdrawn from circulation in 2011. Version 1.0 samples found after this date seem to have been improperly removed or were no longer accessible to the attackers for removal.

This report is based primarily on our analysis of Regin version 1.0. We also touch on version 2.0, for which we only recovered 64-bit files.

Symantec has assigned these version identifiers as they are the only two versions that have been acquired. Regin likely has more than two versions. There may be versions prior to 1.0 and versions between 1.0 and 2.0.

Target profile

The Regin operators do not appear to focus on any specific industry sector. Regin infections have been observed in a variety of organizations, including private companies, government entities, and research institutes.

Infections are also geographically diverse, having been identified mainly in 10 different regions.

Infection vector

The infection vector varies among targets. A reproducible infection vector is unconfirmed at time of writing. Targets may be tricked into visiting spoofed versions of well-known websites and the threat may be installed through a web browser or by exploiting an application. On one computer, log files show that Regin originated from Yahoo! Instant Messenger through an unconfirmed exploit.

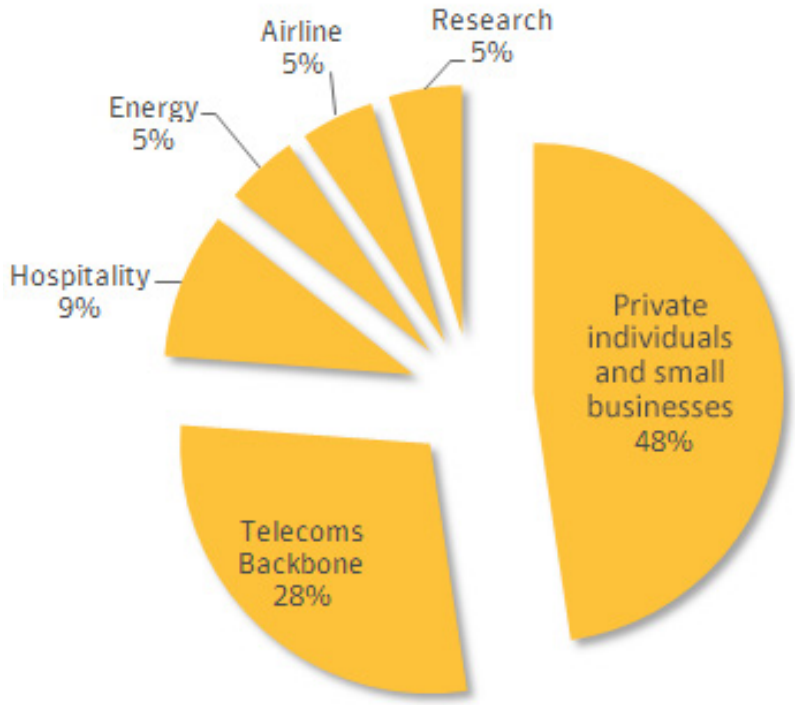


Figure 1. Confirmed Regin infections by sector

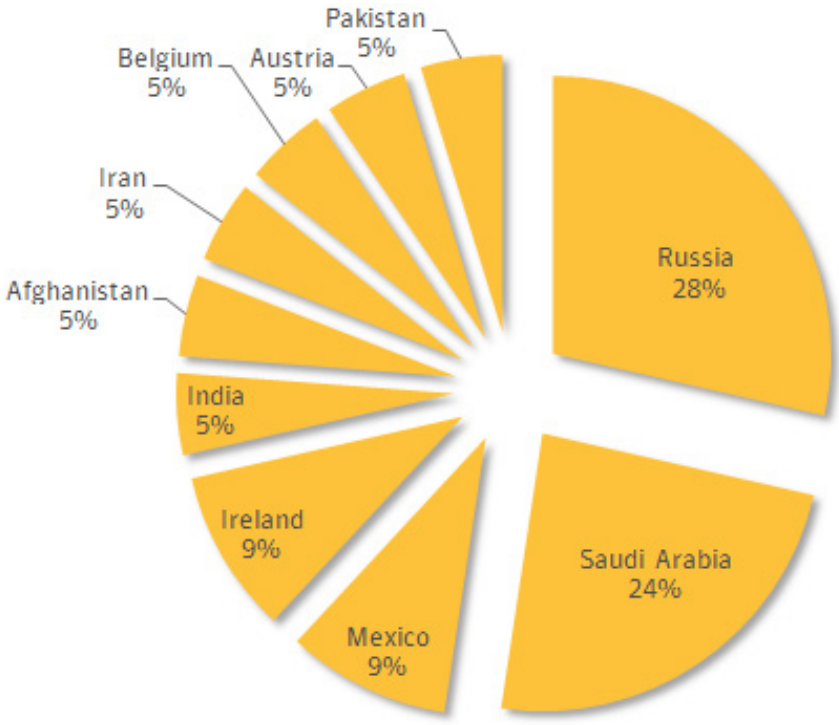


Figure 2. Confirmed Regin infections by country

Symantec

ARCHITECTURE

> “The initial Stage 1 driver is the only plainly visible code on the computer. All other stages are stored as encrypted data blobs...”

Architecture

Regin has a six-stage architecture. The initial stages involve the installation and configuration of the threat's internal services. The later stages bring Regin's main payloads into play. This section presents a brief overview of the format and purpose of each stage. The most interesting stages are the executables and data files stored in Stages 4 and 5. The initial Stage 1 driver is the only plainly visible code on the computer. All other stages are stored as encrypted data blobs, as a file or within a non-traditional file storage area such as the registry, extended attributes, or raw sectors at the end of disk.

Table 1. The six stages of Regin

Stages	Components
Stage 0	Dropper. Installs Regin onto the target computer
Stage 1	Loads driver
Stage 2	Loads driver
Stage 3	Loads compression, encryption, networking, and handling for an encrypted virtual file system (EVFS).
Stage 4	Utilizes the EVFS and loads additional kernel mode drivers, including payloads.
Stage 5	Main payloads and data files

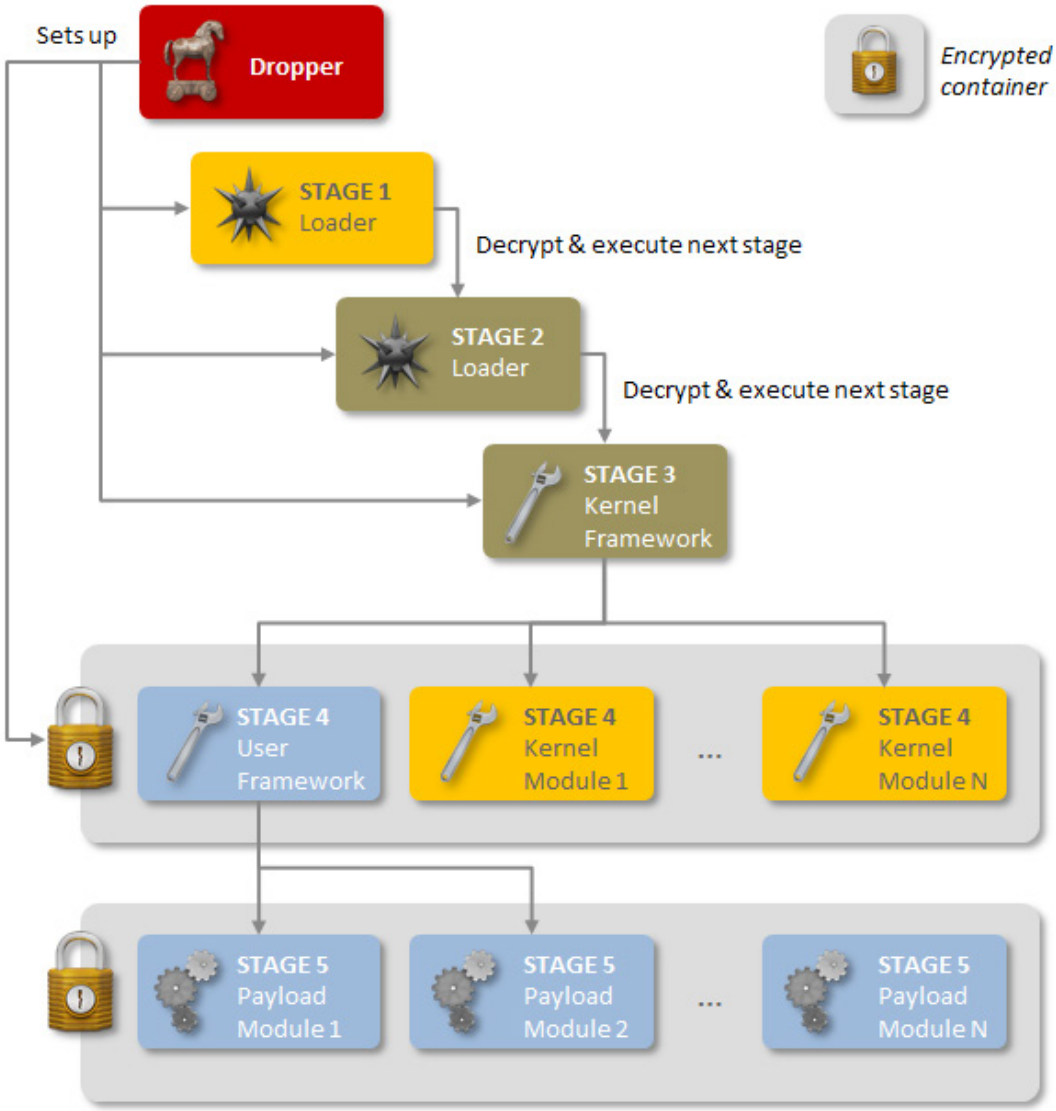


Figure 3. Regin's architecture

Stage 0 (dropper)

Symantec Security Response has not obtained the Regin dropper at the time of writing. Symantec believes that once the dropper is executed on the target's computer, it will install and execute Stage 1. It's likely that Stage 0 is responsible for setting up various extended attributes and/or registry keys and values that hold encoded versions of stages 2, 3, and potentially stages 4 and onwards. The dropper could be transient rather than acting as an executable file and may possibly be part of the infection vector exploit code.

Stage 1

Stage 1 is the initial load point for the threat. There are two known Stage 1 file names:

- usbclass.sys (version 1.0)
- adpu160.sys (version 2.0)

These are kernel drivers that load and execute Stage 2. These kernel drivers may be registered as a system service or may have an associated registry key to load the driver while the computer is starting up.

Stage 1 simply reads and executes Stage 2 from a set of NTFS extended attributes. If no extended attributes are found, Stage 2 is executed from a set of registry keys.

Stage 2

Stage 2 is a kernel driver that simply extracts, installs and runs Stage 3. Stage 2 is not stored in the traditional file system, but is encrypted within an extended attribute or a registry key blob.

Stage 2 can be found encrypted in:

Extended attribute

- %Windir%
- %Windir%\fonts
- %Windir%\cursors (possibly only in version 2.0)

Registry subkey

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase (possibly only in version 2.0)

This stage can also hide running instances of Stage 1. Once this happens, there are no remaining plainly visible code artifacts. Similar to previous stages, Stage 2 finds and loads an encrypted version of Stage 3 from either NTFS extended attributes or a registry key blob.

Stage 2 can also monitor the state of the threat. This stage drops the file msrdc64.dat, which appears to always be 512 bytes in size. The first two bytes are used and the remaining bytes are set to zero. The second byte indicates the exclusive maximum number of instances allowed to run, which is set to two. This means no more than one instance should run at any time. The first byte indicates how many instances were run or attempted to run. Therefore, the potential combinations for the first two bytes are:

- 00 02 (the threat is not running)
- 01 02 (the threat is running)
- 02 02 (the threat was running and a second instance has started).

Stage 3

Stage 3 is a kernel mode DLL and is not stored in the traditional file system. Instead, this file is encrypted within an extended attribute or registry key blob.

Stage 3 can be found in the following locations:

Extended attribute

- %Windir%\system32
- %Windir%\system32\drivers

Registry subkey

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}

The file is six to seven times the size of the driver in Stage 2. In addition to loading and executing Stage 4, Stage 3 offers a framework for the higher level stages.

Stages 3 and above are based on a modular framework of code modules. These modules offer functions through a private, custom interface. Each file in stages 3 and above can "export" functionality to other parts of Regin.

In the case of Stage 3, the following primitives are offered:

- The orchestrator, which parses custom records found in the appended data of the executable files for stages 3 and above. These records contain a list of Regin functionalities to be executed. A record starts with the number 0xD912FEAB (little-endian ordering)
- Compression and decompression routines
- Encryption and decryption routines
- Routines to retrieve storage locations of higher-level (Stage 4) components
- Routines to handle an encrypted virtual file system used by Stage 4
- Network primitives

These primitives are provided through a custom export methodology.

Export methodology

The Stage 3 DLL exports a wide range of functionality through a custom export methodology. The interface used to export functionality does not make use of the traditional Windows DLL export mechanism by name or ordinal.

Exported Regin methods are referenced by a tuple consisting of a major and minor number. Stage 3 exports hundreds of methods, organized into 12 different major groups. The numbers used vary across versions. We acquired artifacts using two different numbering schemes. Table 2 is an example listing.

With Regin's modular nature, Stage 4 kernel modules and Stage 5 user modules (payloads) can provide functionality and export routines using the same major and minor numbering scheme.

Table 2. An example of Regin's methods organized into 12 groups

Major	Functionality
0001h	Core
000Dh	Compression, decompression
000Fh	Encryption, decryption
003Dh	EVFS handling
0007h	Container management
000Bh	Log management
0033h	Loader
0011h	Network
0013h	Network
C373h	TCP command-and-control (C&C)
0019h	UDP C&C
0009h	C&C Processor

Stage 4

The files for Stage 4, which are loaded by Stage 3, consist of a user-mode orchestrator and multiple kernel payload modules. They are stored in two EVFS containers as files:

- %System%\config\SystemAudit.Evt: Contains Stage 4 kernel drivers, which constitute the kernel mode part of Regin's payload.
- %System%\config\SecurityAudit.Evt: Contains a user mode version of Stage 3. The files are injected into services.exe.

When the attackers who operated Regin cleaned up compromised computers once they were finished with them, they often failed to remove Stage 4 and 5 artifacts from the system.

Stage 4 also uses the same export methodology described in Stage 3.

Stage 5

Stage 5 consists of the main Regin payload functionality. The files for Stage 5 are injected into services.exe by Stage 4.

Stage 5 files are EVFS containers containing other files:

- %System%\config\SystemLog.evt: Contains Stage 5 user mode DLLs. They constitute Regin's payload.
- %System%\config\SecurityLog.evt: Contains Stage 5 data files, used by the Stage 4 and 5 components to store various data items
- %System%\config\ApplicationLog.evt: Another Stage 5 log container, which is referenced by Stage 5 data files
- %Windir%\ime\imesc5\dicts\pintlgbp.imd (version 2.0)
- %Windir%\ime\imesc5\dicts\pintlgbs.imd (version 2.0)

Regin's payload involves the DLLs contained in the SystemLog.evt EVFS container. The payload functionality differs depending on the targeted computer. Custom payload files will likely be delivered for each specific environment. Example payload functionality seen to date includes:

- Sniffing low-level network traffic
- Exfiltrating data through various channels (TCP, UDP, ICMP, HTTP)
- Gathering computer information
- Stealing passwords
- Gathering process and memory information
- Crawling through the file system
- Low level forensics capabilities (for example, retrieving files that were deleted)
- UI manipulation (remote mouse point & click activities, capturing screenshots, etc.)
- Enumerating IIS web servers and stealing logs
- Sniffing GSM BSC administration network traffic

Encrypted virtual file system containers

Regin stores data files and payloads on disk in encrypted virtual file system files. Such files are accessed by the major routines 3Dh. Files stored inside EVFS containers are encrypted with a variant of RC5, using 64-bit blocks and 20 rounds. The encryption mode is reverse cipher feedback (CFB).

Known extensions for EVFS containers are *.evt and *.imd. The structure of a container is similar to the FAT file system. One major difference is that files do not have a name; instead, they're identified using a binary tag. The tag itself is the

Figure 4. Physical layout of an EVFS container

concatenation of a major number and a minor number. The major number typically indicates the major function group that will handle the file.

A container starts with the header in Table 3 (little-endian ordering).

The header is followed by the file entry table (Table 4). Each file entry is 13h+taglen bytes long.

The sectors follow (Table 5). A sector of sectsize bytes starts with a DWORD pointing to the next sector (if the file does not fit within a single sector), followed by sectsize-4 bytes of payload data.

As explained above, the files are encrypted. Other layers of encryption and compression may also be in place, although those would be handled by higher level components.

Table 3. The container's header

Offset	Type	Description
00h	WORD	Sector size in bytes
02h	WORD	Maximum sector count
04h	WORD	Maximum file count
06h	BYTE	File tag length (taglen)
07h	DWORD	Header CRC
0Bh	DWORD	File table CRC
0Fh	WORD	Number of files
11h	WORD	Number of sectors in use
13h	-	Sector-use bitmap

Table 4. The container's file entry table

Offset	Type	Description
00h	DWORD	CRC
04h	DWORD	File offset
08h	DWORD	Offset to first sector holding the file data
0Ch	BYTE[taglen]	File tag

Table 5. The container's sectors

Offset	Type	Description
00h	DWORD	Next sector offset, or 0
04h	BYTE[sectsize-4]	Data

Command-and-control operations

Regin's C&C operations are extensive. These backchannel operations are bidirectional, which means either the attackers can initiate communications with compromised computers on the border network or the compromised computers can initiate communications with the attacker. Furthermore, compromised computers can serve as a proxy for other infections and command and control can also happen in a peer-to-peer fashion. All communications are strongly encrypted and can happen in a two-stage fashion where the attacker may contact a compromised computer using one channel to instruct it to begin communications on a different channel. Four transport protocols are available for C&C:

- ICMP: Payload information can be encoded and embedded in lieu of legitimate ICMP/ping data. The string 'shit' is scattered in the packet for data validation. In addition, CRC checks use the seed '31337'.
- UDP: Raw UDP payload
- TCP: Raw TCP payload
- HTTP: Payload information can be encoded and embedded within cookie data under the names SESSID, SMSWAP, TW, WINKER, TIMESET, LASTVISIT, AST.NET_SessionId, PHPSESSID, or phpAds_d. This information can be combined with another cookie for validation under the names USERIDTK, UID, GRID, UID=PREF=ID, TM, __utma, LM, TMARK, VERSION, or CURRENT

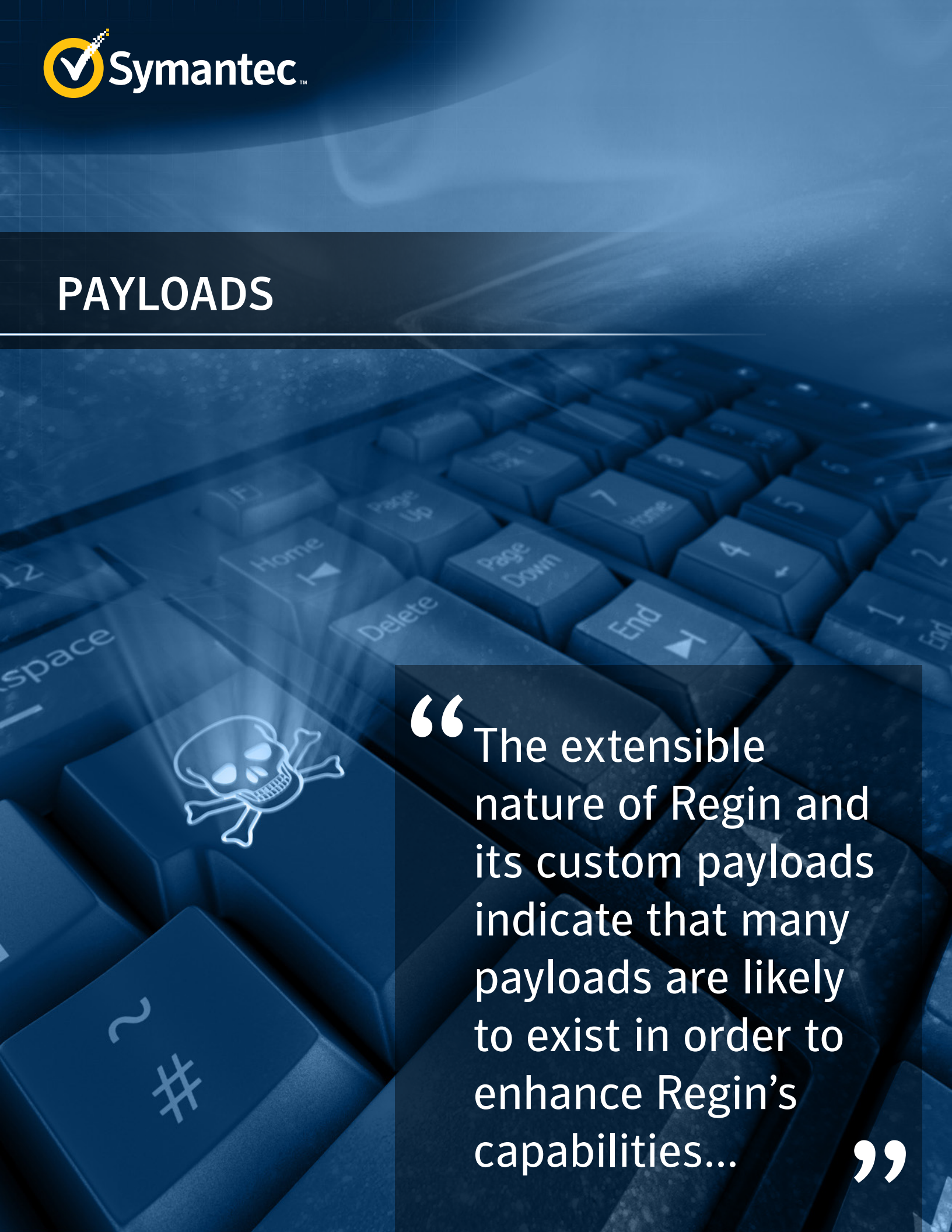
The C&C operations are undertaken by various modules, including major groups C373h, 19h, 9, as well as Stage 5 payloads, such as C375h and 1Bh.

Logging

Regin logs data to the ApplicationLog.dat file. This file is not an encrypted container, but it is encrypted and compressed.

Symantec

PAYLOADS



> “The extensible nature of Regin and its custom payloads indicate that many payloads are likely to exist in order to enhance Regin’s capabilities...”

Payloads

Regin can be distributed with various payload modules or receive payload modules after infection. The extensible nature of Regin and its custom payloads indicate that many additional payloads are likely to exist in order to enhance Regin's capabilities. Furthermore, we have found data files accompanying payload modules that have not been recovered. The following table describes the Stage 4 kernel payload modules and Stage 5 user mode payload modules, which we have seen several variants of Regin use.

Table 6. Regin's stage 4 kernel payload modules and stage 5 user mode payload modules

File type	Major	Description
SYS	0003	Driver
SYS	C433	Rootkit
SYS	C42B	PE loader
SYS	C42D	DLL injection
SYS	C3C3	Network packet filter driver similar to the WinPCap (protocol filter version 3.5) Used to set TCP and UDP pass-through filters and to bypass firewalls. Executes BPF (Berkeley Packet Filter) bytecode, stored in Stage 5 data files.
SYS	4E69	Network port blocker
DLL	C363	Network packet capture
DLL	4E3B	Retrieve proxy information for a web browser (Internet Explorer, Netscape, Firefox) through registry or configuration files (for example, prefs.js, refs.js, etc.) Enumerate sessions and user accounts
DLL	290B	Password stealer • Windows Explorer credentials • Windows Explorer pstore records • Internet Explorer LegacySettings • Data for a Winlogon notification package named "cryptpp"
DLL	C375	C&C HTTP/cookies
DLL	C383	SSL communications
DLL	C361	Supporting cryptography functions
DLL	001B	ICMP backchannel
DLL	C399	Record builder for ApplicationLog.Evt
DLL	C39F	Processes file: %Temp%\~b3y7f.tmp
DLL	C3A1	Miscellaneous functions
DLL	28A5	Miscellaneous functions
DLL	C3C1	Miscellaneous functions
DLL	C3B5	Gather system information • CPUMemory • Drives and shares • Devices • Windows information (including type, version, license info, owner info) • Installed software • Running processes (through HKEY_PERFORMANCE_DATA id 230) • Services • Schedules tasks and jobs • Running desktop sessions • User accounts information • System's auditing rules/policy • System time and Windows install time

DLL	C36B	UI manipulation • Capture screenshots • Log keystrokes • Lock the workstation/input Ctrl-Alt-Del • Click functionality (through three commands: go, click & release, return to original position) • End processes
DLL	C351	File system exploration primitives and forensic level exploration including a raw NTFS parser • Get miscellaneous file information and properties • Browse directories • Read and write files • Move and copy files • Read and recover partially or fully deleted files • Compute file hashes
DLL	2B5D	Process and module manipulation • Read processes and modules • Processes running times, quotas, privileges • Skip Russian or English Microsoft files when scanning • Check for newly introduced PE files in the last two days
DLL	C3CD	Enumerate TCP/IP interfaces from %System%\CurrentControlSet\Services\Tcpip\Linkage\bind
DLL	C38F	TCPDump utility
DLL	C3C5	Libnet binary
DLL	27E9	IIS web server log theft Enumeration through COM objects to find IIS logs. Ability to retrieve partial or complete log information. • Partial: Log type, last log, older log timestamps • Complete: Entire log data is exfiltrated

The IIS web server log stealing module, 27E9h, is an example of a payload module that was installed after the initial infection and was specifically deployed for a particular target.

64-bit version

Only a small amount of the 64-bit Regin files have been recovered. These samples may represent version 2.0 or their differences may possibly be solely specific to 64-bit versions of Regin. We also recovered files from infected computers that may or may not be associated with 64-bit Regin, including several variants of svcsstat.exe, a file that aims to retrieve binary data over pipes or sockets and execute the data.

File names

The recovered files do not appear to fundamentally vary from their 32-bit counterparts, apart from a few noteworthy differences.

The 32-bit and 64-bit versions of Regin use different file names. These differences are shown in the first section of this paper as well as in the appendix. Most importantly, in the 64-bit version of Regin, the names of containers are changed:

- PINTLGBP.IMD replaces SystemLog.Evt
- PINTLGBPS.IMD replaces SecurityLog.Evt

Stage differences

The 64-bit version of Regin's Stage 1 (wshnetc.dll) is no longer a kernel mode driver, as drivers under 64-bit Windows must be signed. Instead, Stage 1 is a user mode DLL loaded as a Winsock helper when the computer is starting up. Rather than loading Stage 2 from an NTFS extended attribute, Stage 1 looks for the last partition (in terms of

physical location) on disk and searches for the payload in the raw sectors in this area of the disk.

The 64-bit Regin's Stage 3 has not been recovered. We believe that it may not exist, as the 32-bit version is a driver. Stage 4 is an orchestrator just like its 32-bit counterpart and it uses the same major and minor values to export functionality.

Stage 5 uses the following filenames:

- %Windir%\IME\IMESC5\DICTS\PINTLGBP.IMD contains Stage 5 user payloads, replacing SystemLog.Evt in the 32-bit version
- %Windir%\IME\IMESC5\DICTS\PINTLGBS.IMD contains Stage 5 data files, replacing SecurityLog.Evt in the 32-bit version
- The equivalent files for SystemAudit.Evt and SecurityAudit.Evt were not recovered

No Stage 5 payload modules have been recovered.

Conclusion

Regin is a highly-complex threat which has been used for large-scale data collection or intelligence gathering campaigns. The development and operation of this threat would have required a significant investment of time and resources. Threats of this nature are rare and are only comparable to the Stuxnet/Duqu family of malware. The discovery of Regin serves to highlight how significant investments continue to be made into the development of tools for use in intelligence gathering. Many components of Regin have still gone undiscovered and additional functionality and versions may exist.

Protection

Regin components are detected as Backdoor.Regin.

Symantec™

APPENDIX

Appendix

Data files

Regin's data files are classified as Stage 5 components and are contained in an EVFS container.

Table 7. Data files used by Stage 4's framework DLL

Major	Minor	Description
0001	-	-
000D	-	-
000F	01	High-entropy blobs, cryptographic data
	02	High-entropy blobs, cryptographic data
003D	-	-
0007	-	-
000B	01	Contains a path to the log file. Typically, %System\config\ApplicationLog.Evt
	02	Small 8 byte files
0033	01	A single DWORD, such as 111Ch
	03	A single DWORD, such as 1114h
0011	-	-
0013	01	Unknown list of records
	02	A single byte, such as 3
C373	01	BPF bytecode for the netpcap driver—allows UDP passthrough
	02	A WORD value, such as 1
0019	01	BPF bytecode for the netpcap driver—allows TCP passthrough
	02	A WORD value, such as 1
0009	00	A single DWORD, such as 11030B15h
	01	Contains C&C location information
	02	C&C routines to be executed: • (C375, 1) param= 08 02 • (19, 1) param= 44 57 58 00 • (C373, 1) param= 08 02 • (1B, 1) param= 20 00
	03	Routines to be executed • (4E69, 2) • (19, 2) • (1B, 2) • (C373, 2)(• C375, 2) • (C383, 2)(C363, 2)
	07	RC5 key used to decrypt command-and-control packets
	09	Unknown data
	0B	Unknown data
	12	A single byte, such as 1
	17	Unknown data

As the data files are stored in a container, they do not have names. Just like Stage 5 modules, they are referenced by their filetag, which is the aggregation of the major and minor identifiers. The major identifier indicates which major routine group likely handles or creates the file.

Not all data files have been recovered, so the information remains incomplete.

Data files associated with Stage 4 kernel modules have not been recovered

Table 8 lists recovered data files used by Stage 5 modules.

The associated modules that supposedly manipulate those data files were not recovered.

Table 8. Data files used by Stage 5's modules (payloads)

Major	Minor	Description
C363	02	6 bytes (01 00 00 00 00 00)
4E3B	-	
290B	-	
C375	01	Dword (1)
	02	Dword (0)
C383	01	Dword (1)
	02	Dword (0)
	10	64 bytes (512 bits)Diffie Hellman, p (prime)
	11	Byte (2)Diffie Hellman, g (generator)
C361	10	File containing timestamps and high entropy dataUnclear
	11	Dword (E10h)
	12	Dword (2)
001B	-	
C399	-	
C39F	00	Small file, 18h bytes, low entropy
	01	Unencrypted unicode path, %Temp%\~B3Y7F.tmp
C3A1	01	Small file, 6 bytes (08 01 00 00 00 01)
28A5	02	Small file, 18h bytes, unknown
C3C1	-	-
C3B5	-	-
C36B	-	-
C351	-	-
2B5D	-	-
C3CD	-	-
C38F	-	-
C3C5	-	-
27E9	-	-

Table 9. Orphaned data files

Major	Minor	Description
4E25	00	Byte (1)
	01	Byte (2)
28A4	00	Unknown
	02	Small file, 8 bytes (01 00 00 00 00 00 00 00)
DEAB	01	Small file, 8 bytes (00 00 01 01 04 00 00 00)

Indicators of compromise

The following details can be used to help determine whether you have been impacted by this threat.

File MD5s

2c8b9d2885543d7ade3cae98225e263b

4b6b86c7fec1c574706cecedf44abded

187044596bc1328efa0ed636d8aa4a5c

06665b96e293b23acc80451abb413e50

d240f06e98c8d3e647cbf4d442d79475

6662c390b2bbbd291ec7987388fc75d7

ffb0b9b5b610191051a7bdf0806e1e47

b29ca4f22ae7b7b25f79c1d4a421139d

1c024e599ac055312a4ab75b3950040a

ba7bb65634ce1e30c1e5415be3d1db1d

b505d65721bb2453d5039a389113b566

b269894f434657db2b15949641a67532

bfbe8c3ee78750c3a520480700e440f8

File names/paths

usbclass.sys

adpu160.sys

msrdc64.dat

msdcsvc.dat

%System%\config\SystemAudit.Evt

%System%\config\SecurityAudit.Evt

%System%\config\SystemLog.evt

%System%\config\ApplicationLog.evt

%Windir%\ime\imesc5\dicts\pintlgbs.imd

%Windir%\ime\imesc5\dicts\pintlgbp.imd

%Windir%\system32\winhttpc.dll

%Windir%\system32\wshnetc.dll

%Windir%\SysWow64\wshnetc.dll

%Windir%\system32\svcstat.exe

%Windir%\system32\svcsstat.exe

Extended attributes

%Windir%

%Windir%\cursors

%Windir%\fonts

%Windir%\System32

%Windir%\System32\drivers

Registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 21,500 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com