McAfee Labs

Rovnix Downloader Updated with SinkHole and Time Checks

By Asheer Malhotra on Dec 09, 2015

Like 19 Share 29 G+1 1 Tweet Email

McAfee Labs has found that the latest Rovnix downloader now comes with the capability to check for the sinkholing of its control servers. This relatively new technique makes it difficult to detect the malware—especially on behavior-based malware detection systems. The malware checks for sinkholing of its control servers before each network communication session and does not initiate its malicious activities—such as downloading and running the malicious payload(s)—if it thinks the Domain Name Service (DNS) records have been sinkholed. The downloader also uses an uncommon technique to perform a timing check to decide whether it should perform its malicious activities.

About Rovnix

Rovnix is a malware family that has been around since 2011. It hijacks the boot sector by infecting the VBR and NT LDR to persist on the target system. Its malicious capabilities include:

- Stealing banking information from victims by infecting browser processes.
- Stealing other passwords from the victim's system.
- Stealing Bitcoins from the target's wallets.

The Rovnix malware family is modular in nature. It can:

- Update its control servers after it has infected the target system.
- Download new plug-ins, giving it the ability to carry out new malicious activities in the future.
- Infect both 32- and 64-bit systems with corresponding DLLs and bootkit infection drivers and code.

Sinkholing

DNS translates domain names such as www.website_name.com to IP addresses that can be used by networking applications such as browsers to send and receive content from a web server. For applications that use domain names, DNS requests are the first step in establishing communication with web-based servers. Any malicious application that uses a domain name for its control servers needs to contact a DNS server to translate the domain name into a valid IP address for the servers.

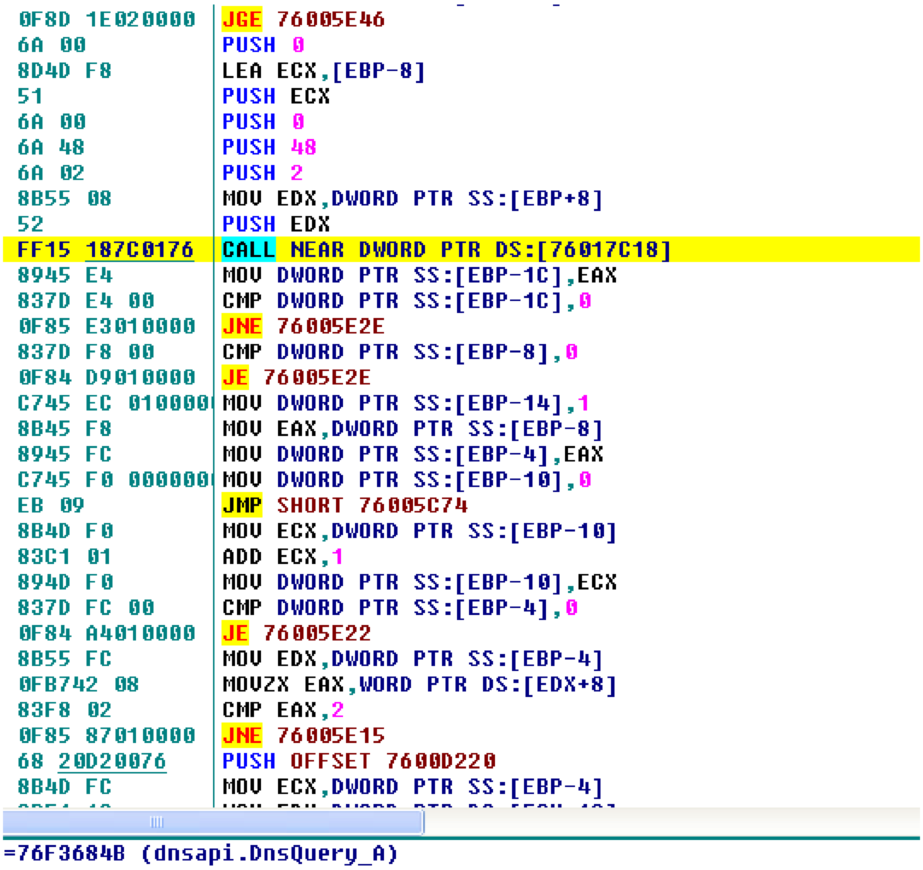
Sinkholing intercepts the DNS request by the malware for a control server and responds with a spoofed address instead of the valid server IP. This disrupts the communication of the malware with its control server and has several advantages. The malware can no longer:

- Download commands to execute on the target system.
- Download new modules or malware to execute on the target system.
- Exfiltrate stolen data from the target system.
- Provide its status to the control server (in the case of botnets).
- Send system statistics to the control server (such as system type, antimalware installed, etc.).
- Download encryption keys from the control server, thus preventing the target's files from being encrypted (in the case of ransomware).

Sinkholing has been used to disrupt a wide variety of malware campaigns including Trojans, botnets, ransomware, and other threats.

Sinkhole Detection Technique

In a simple yet effective technique, the malware fetches the DNS name server records for the control server it attempts to contact.



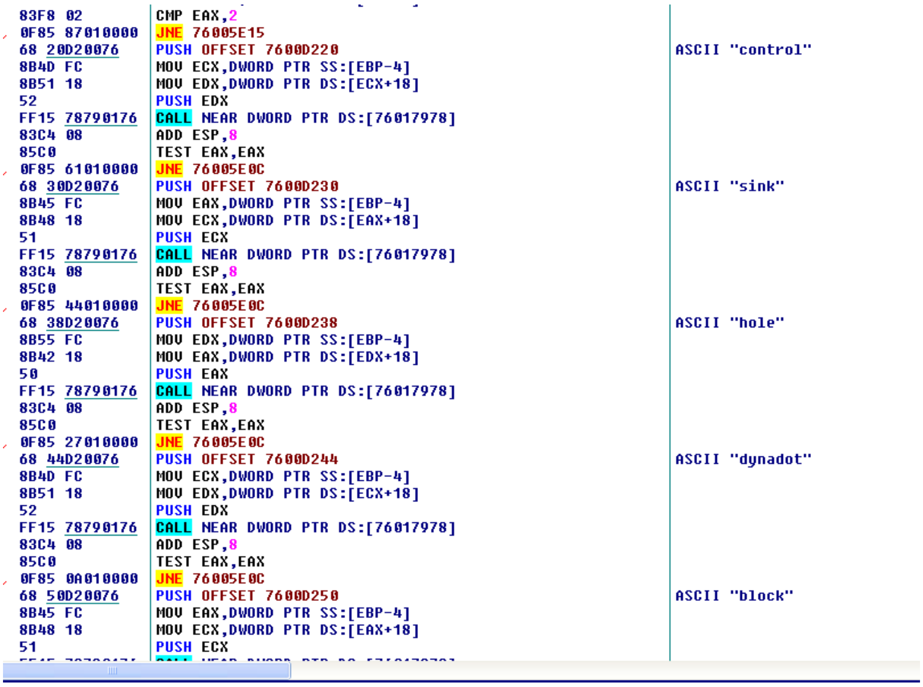
```
0F8D 1E020000   JGE 76005E46
6A 00           PUSH 0
8D4D F8         LEA ECX,[EBP-8]
51              PUSH ECX
6A 00           PUSH 0
6A 48           PUSH 48
6A 02           PUSH 2
8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
52              PUSH EDX
FF15 187C0176   CALL NEAR DWORD PTR DS:[76017C18]
8945 E4         MOV DWORD PTR SS:[EBP-1C],EAX
837D E4 00      CMP DWORD PTR SS:[EBP-1C],0
0F85 E3010000   JNE 76005E2E
837D F8 00      CMP DWORD PTR SS:[EBP-8],0
0F84 D9010000   JE 76005E2E
C745 EC 010000  MOV DWORD PTR SS:[EBP-14],1
8B45 F8         MOV EAX,DWORD PTR SS:[EBP-8]
8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
C745 F0 000000  MOV DWORD PTR SS:[EBP-10],0
EB 09           JMP SHORT 76005C74
8B4D F0         MOV ECX,DWORD PTR SS:[EBP-10]
83C1 01         ADD ECX,1
894D F0         MOV DWORD PTR SS:[EBP-10],ECX
837D FC 00      CMP DWORD PTR SS:[EBP-4],0
0F84 A4010000   JE 76005E22
8B55 FC         MOV EDX,DWORD PTR SS:[EBP-4]
0FB742 08       MOVZX EAX,WORD PTR DS:[EDX+8]
83F8 02         CMP EAX,2
0F85 87010000   JNE 76005E15
68 20D20076     PUSH OFFSET 7600D220
8B4D FC         MOV ECX,DWORD PTR SS:[EBP-4]

=76F3684B (dnsapi.DnsQuery_A)
```

DNSQuery call to fetch DNS name servers.

The name server value(s) are then checked against a list of keywords that might indicate that the DNS name server records for the control server have been sinkholed. The malware checks for the following keywords in the DNS name server record values:

- control
- sink
- hole
- dynadot
- block
- trojan
- abuse
- virus
- malw
- hack
- black
- spam
- anti

- googl



```
83F8 02           CMP EAX,2
0F85 87010000     JNE 76005E15
68 20D20076       PUSH OFFSET 7600D220                                    ASCII "control"
8B4D FC           MOV ECX,DWORD PTR SS:[EBP-4]
8B51 18           MOV EDX,DWORD PTR DS:[ECX+18]
52                PUSH EDX
FF15 78790176     CALL NEAR DWORD PTR DS:[76017978]
83C4 08           ADD ESP,8
85C0              TEST EAX,EAX
0F85 61010000     JNE 76005E0C
68 30D20076       PUSH OFFSET 7600D230                                    ASCII "sink"
8B45 FC           MOV EAX,DWORD PTR SS:[EBP-4]
8B48 18           MOV ECX,DWORD PTR DS:[EAX+18]
51                PUSH ECX
FF15 78790176     CALL NEAR DWORD PTR DS:[76017978]
83C4 08           ADD ESP,8
85C0              TEST EAX,EAX
0F85 44010000     JNE 76005E0C
68 38D20076       PUSH OFFSET 7600D238                                    ASCII "hole"
8B55 FC           MOV EDX,DWORD PTR SS:[EBP-4]
8B42 18           MOV EAX,DWORD PTR DS:[EDX+18]
50                PUSH EAX
FF15 78790176     CALL NEAR DWORD PTR DS:[76017978]
83C4 08           ADD ESP,8
85C0              TEST EAX,EAX
0F85 27010000     JNE 76005E0C
68 44D20076       PUSH OFFSET 7600D244                                    ASCII "dynadot"
8B4D FC           MOV ECX,DWORD PTR SS:[EBP-4]
8B51 18           MOV EDX,DWORD PTR DS:[ECX+18]
52                PUSH EDX
FF15 78790176     CALL NEAR DWORD PTR DS:[76017978]
83C4 08           ADD ESP,8
85C0              TEST EAX,EAX
0F85 0A010000     JNE 76005E0C
68 50D20076       PUSH OFFSET 7600D250                                    ASCII "block"
8B45 FC           MOV EAX,DWORD PTR SS:[EBP-4]
8B48 18           MOV ECX,DWORD PTR DS:[EAX+18]
51                PUSH ECX
```

String comparisons against DNS name server values.

Once the DNS name servers pass the sinkhole checks, the malware downloads various modules to steal information from the victim's machine.

Domains Contacted

All of the domains that follow are control servers used to download malicious plug-ins/modules. The malware starts by contacting the first server listed. If it cannot contact the first server, it tries contacting the next server listed, and so on.

The domains listed are for MD5: 7ce075e3063782f710d47c77ddfa1261

- transliteraturniefabriki.com: the first control server for communication and downloading additional plugins.
- tornishineynarkkek2.org: a backup server. The domain has a history of switching IP addresses.
- upmisterfliremsnk.net: a backup server. The domain also has a history of switching IP addresses.
- itnhi4vg6cktylw2.onion: the last server. If none of the other control servers can be contacted, then the malware establishes a connection with this onion address.

Additional control domains seen in other Rovnix downloaders:

- lastoooooomene2ie2e.com
- ecloud86.com, ecloud87.com, ecloud88.com, ecloud89.com, ecloud90.com, ecloud91.com
- srvdexpress3.com, srvdexpress4.com, srvdexpress5.com,

srvdexpress6.com, srvdexpress7.com
- elorfans2.com, elorfans3.com, elorfans4.com, elorfans5.com, elorfans6.com
- tornishineynarkkek.org, tornishineynarkkek3.org
- mediacontent.us, mediacontent2.us, mediacontent3.us
- romnsiebabanahujtr.org, romnsiebabanahujtr2.org, romnsiebabanahujtr3.org
- pg7iuaqu5b7fq36o.onion
- j7t4lg23tdhag3fn.onion
- c2bbagrsvbs2v6a7.onion
- hbs63zj7mwj5g6w7.onion

IP Addresses Hosting the Domains

Multiple domains in the control server list share the same IP address, indicating that the malicious actor has control of the IPs hosting the domains. For example, the following domains share the same IP:

- lastooooomene2ie2e.com and transliteraturniefabriki.com
- tornishineynarkkek.org, tornishineynarkkek2.org and upmisterfliremsnk.net
- ecloud88.com and ecloud89.com
- srvdexpress3.com, srvdexpress4.com and srvdexpress5.com
- elorfans3.com and elorfans4.com

Timing Checks

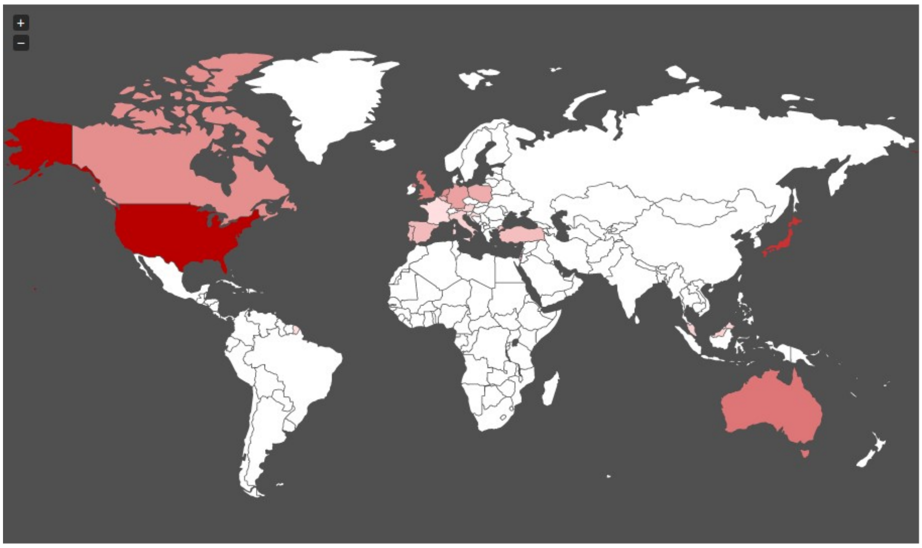
The malware also does a time check using standard Network Time Protocol (NTP) servers to decide whether to proceed with its malicious activities. The check compares the times received from the control server and public time servers. If the time elapsed exceeds a certain threshold, the malware sleeps for a period before checking the times again. The time stamp might be fetched from the public NTP servers because many malware analysis systems can spoof local system time to trick the malware into running its malicious code.

Targets

The downloaders have primarily been encountered in the United States, Canada, Japan, and parts of Europe.

The following map shows a geographic distribution of the

Rovnix downloader:



Geographic distribution of the Rovnix downloader infections.

Conclusion

The newest downloader for Rovnix introduces a new method to detect DNS sinkholing. This technique allows the malware to protect itself by not executing its malicious code if the control server has been sinkholed. Multiple server domains hosted on a single IP also indicate that one attacker might have control of these servers.

The usage of public NTP servers to check the time is a relatively new capability. This technique combats spoofing of local system time used by many dynamic malware detection systems.

MD5 Sums

7ce075e3063782f710d47c77ddfa1261
11f61c60ce548e2148c2f7a2e5f7103c
e8a94f1df66587abd7c91bfcbe5af5d5
fdef7dd0b7cece42042a7baca3859e41
b7d63dcb586ec9a54a91379990dcd804
7123a117c44e8c454f482b675544d1a9
5ea867f5f7c24e0939013faf3ed78535
0131d46686c66e6a4c8d89c3aa03534c
b0bce8bd66a005eff775099563232e64
e0bc0503ccc831c07d6cc4c394b5a409

29ef765145f6dd76cec5cc89c75b44de
a6fd6661c6ac950263ba9a3d4fc55354
19f14a5d5610e51f4985444f3f0e59ed

Yara Rule

The following Yara rule can be used to find samples of the Rovnix downloader:

```
rule rovnix_downloader
{
meta:
author=”Intel Security”
description=”Rovnix downloader with sinkhole checks”

strings:
$sink1=”control”
$sink2 = “sink”
$sink3 = “hole”
$sink4= “dynadot”
$sink5= “block”
$sink6= “malw”
$sink7= “anti”
$sink8= “googl”
$sink9= “hack”
$sink10= “trojan”
$sink11= “abuse”
$sink12= “virus”
$sink13= “black”
$sink14= “spam”
$boot= “BOOTKIT_DLL.dll”
$mz = { 4D 5A }

condition:
$mz in (0..2) and all of ($sink*) and $boot

}
```

Acknowledgements

Thanks to Christiaan Beek, Jonathan Chang, and Sanchit Karve for contributing to this post.

Tags: cybercrime, malware, computer security

Like 19 Share 29 G+1 1 Tweet Email

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

reCAPTCHA

Type the text

Privacy & Terms

Post Comment

Intel Security on Twitter

elSecurity Seasonal charities aren't always what they seem. https://t.co/cNU32iIjoQ #win #SafeHoliday https://t.co/zPP1O6ZiXU

4 hours ago·Reply·Retweet ·Favorite

elSecurity It's the ost scammable time of the year. Teach your family to spot and report online scams: https://t.co/L17Fu4KyCH

7 hours ago·Reply·Retweet ·Favorite

Follow @IntelSecurity

Also Find Us On

About | Subscribe | Contact & Media Requests | Privacy Policy
Legal | FAQ