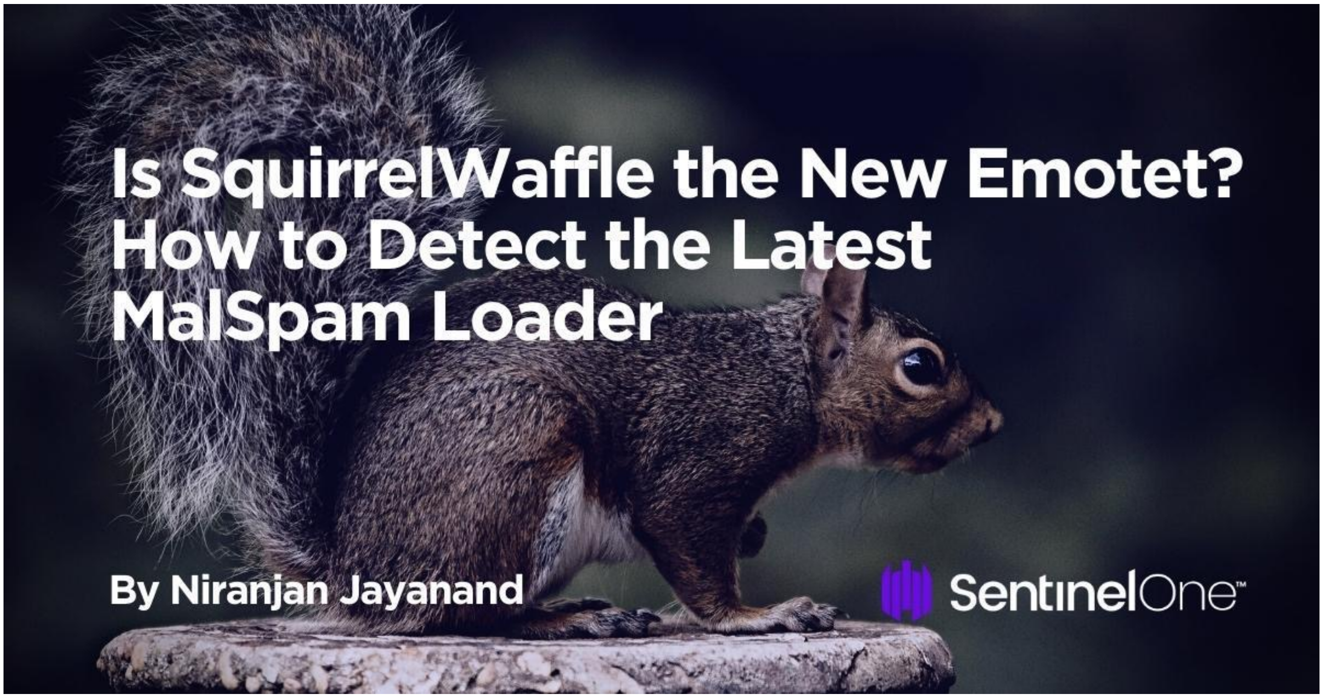
Is SquirrelWaffle the New Emotet? How to Detect the Latest MalSpam Loader

sentinelone.com/blog/is-squirrelwaffle-the-new-emotet-how-to-detect-the-latest-malspam-loader/

November 11, 2021


Is SquirrelWaffle the New Emotet? How to Detect the Latest MalSpam Loader
By Niranjan Jayanand
SentinelOne

Since early September, SentinelLabs has been tracking the rapid rise of a new malware loader that previous researchers have dubbed “SquirrelWaffle”. The tool has been utilized in multiple global attacks since then and is being likened to Emotet in the way it is being used to conduct massive malspam campaigns.

In this post, we explain how SquirrelWaffle works, what to look out for and how to protect your business from the latest malspam loader.

What Is SquirrelWaffle Malware?

SquirrelWaffle is a recent malware loader that is distributed through malspam – malicious spam mail – with the purpose of infecting a device with second-stage malware such as cracked copies of the red teaming tool Cobalt Strike and QakBot, a well-known malware that started life as a simple banking trojan but has since evolved into a multi-functional framework with RAT (Remote Access Trojan)-like capabilities.

Researchers have noted how the infection chain may begin with an email reply chain attack, in which a threat actor neither inserts themselves as a new correspondent nor attempts to spoof someone else’s email address. Instead, the attacker sends the malicious SquirrelWaffle email from a hijacked account belonging to one of the participants. Since the attacker has access to the whole thread, they can tailor their malspam message to fit the context of an ongoing conversation. Given that the recipient likely already trusts the sender, there’s an increased likelihood of the target opening the maldoc or clicking the link. Email reply chain attacks were a hallmark of Emotet campaigns and contributed a great deal to its success.

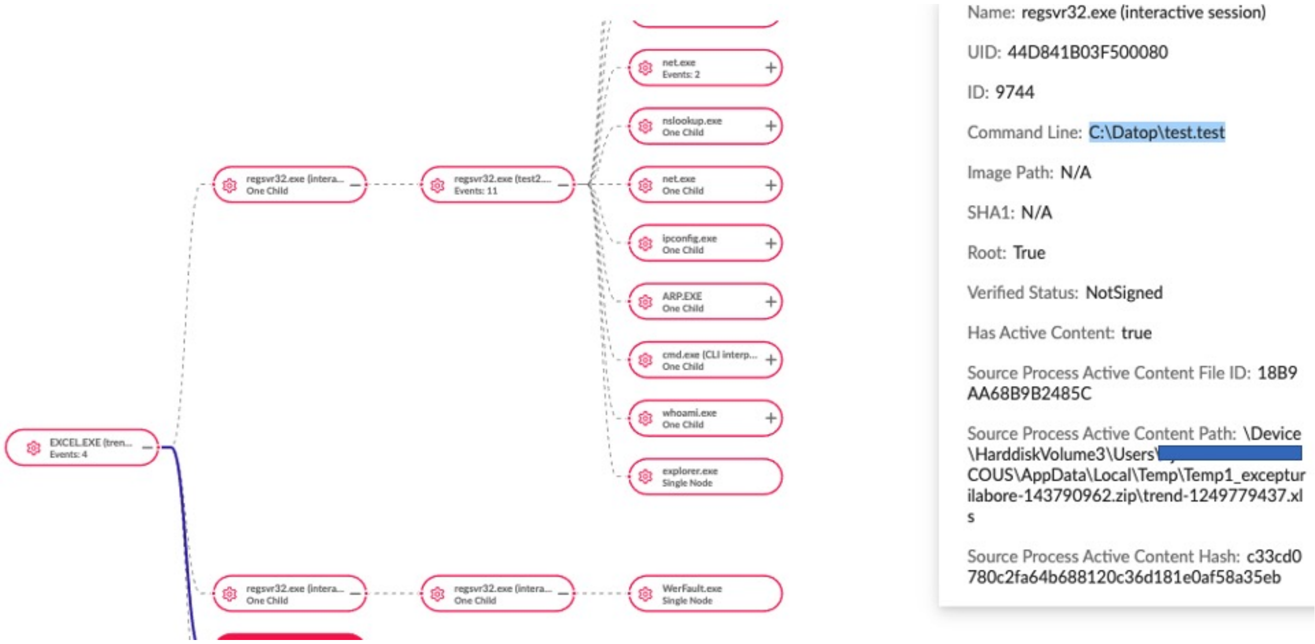
SquirrelWaffle first appeared in early September and defenders have noticed an uptick in incidences of infection since then. SentinelLabs researchers have also noticed that the malware drops unique payloads even from the same infection chain and that file path patterns are continuing to evolve.

How Does SquirrelWaffle Infect Devices?

Initial delivery of SquirrelWaffle as a first stage loader often comes courtesy of a phishing email with either a malicious MS Word or Excel attachment or embedded link leading to a zip-compressed malicious document download. These maldocs contain VBS macros which execute PowerShell to retrieve and launch the SquirrelWaffle loader.

The initial SquirrelWaffle files are written to disk as prescribed by the malicious PowerShell script responsible for their retrieval. For example, early clusters of malicious documents dropped SquirrelWaffle using this set of file names:

```
C:\Datop\test.test
C:\Datop\test1.test
C:\Datop\test2.test
```



Name: regsvr32.exe (interactive session)

UID: 44D841B03F500080

ID: 9744

Command Line: C:\Datop\test.test

Image Path: N/A

SHA1: N/A

Root: True

Verified Status: NotSigned

Has Active Content: true

Source Process Active Content File ID: 18B9AA68B9B2485C

Source Process Active Content Path: \Device\HarddiskVolume3\Users\[redacted]COUS\AppData\Local\Temp\Temp1_excepturilabore-143790962.zip\trend-1249779437.xls

Source Process Active Content Hash: c33cd0780c2fa64b688120c36d181e0af58a35eb

SquirrelWaffle infection following the launch of a poisoned Excel file

Importantly, no two runs of the same malicious document will produce the same SquirrelWaffle payloads. On each execution, the payloads written to disk will have unique hashes.

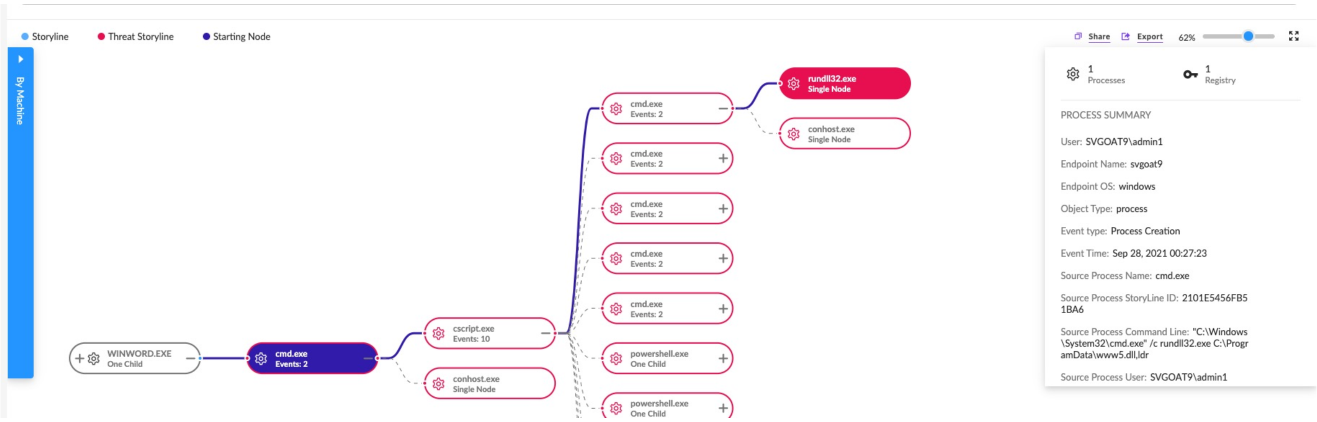
```
"C:\Users\<redact>\AppData\Local\Temp\Temp1_natusut-1501184.zip\grade-2086577786.xls"
C:\Datop\test.test - 8d7089f17bd5706309d7c6986fdd1140d6c5b4b2
C:\Datop\test1.test - 52452f6f0ab73531fe54935372d9c34eb50653d8

"C:\Users\<redact>\OneDrive - folder, Inc\Desktop\grade-2086577786.xls"
C:\Datop\test.test - bce0e9e1c6d2e7b12648ef316748191f10ed8582
C:\Datop\test1.test - 8ba7694017d1cea1d4b73f39479726478df88b20

"C:\Users\\OneDrive - folder, Inc\Desktop\grade-2086577786.xls"
C:\Datop\test.test - 8aec96029b83d3b226c8c83dd90f48946ee97001
C:\Datop\test1.test - 8262cd7029f943a7b6199b5a6c51ec19e085c3b7
```

SquirrelWaffle has been observed using more conventional file name patterns as well, such as those with `.dll` extensions:

```
ww1.dll
ww2.dll
ww3.dll
ww4.dll
ww5.dll
```



PROCESS SUMMARY

User: SVGOAT9\admin1

Endpoint Name: svgoat9

Endpoint OS: windows

Object Type: process

Event type: Process Creation

Event Time: Sep 28, 2021 00:27:23

Source Process Name: cmd.exe

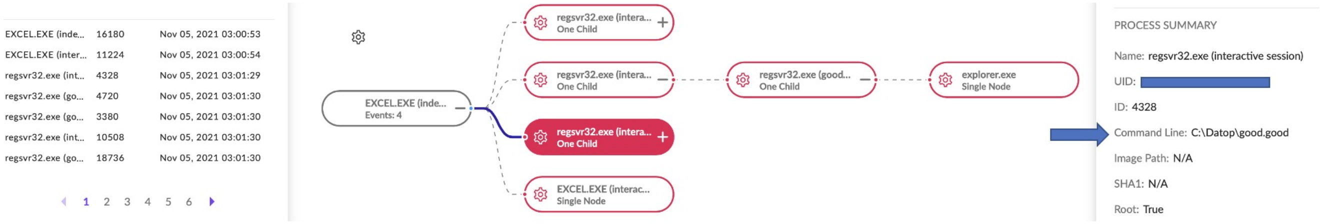
Source Process StoryLine ID: 2101E5456FB51BA6

Source Process Command Line: "C:\Windows\System32\cmd.exe" /c rundll32.exe C:\ProgramData\www5.dll,ldr

Source Process User: SVGOAT9\admin1

In early November, we observed yet another pattern, indicating that the malware authors are continually iterating:

```
good.good
good1.good
good2.good
```



EXCEL.EXE (inde...	16180	Nov 05, 2021 03:00:53
EXCEL.EXE (inter...	11224	Nov 05, 2021 03:00:54
regsvr32.exe (int...	4328	Nov 05, 2021 03:01:29
regsvr32.exe (go...	4720	Nov 05, 2021 03:01:30
regsvr32.exe (go...	3380	Nov 05, 2021 03:01:30
regsvr32.exe (int...	10508	Nov 05, 2021 03:01:30
regsvr32.exe (go...	18736	Nov 05, 2021 03:01:30

PROCESS SUMMARY

Name: regsvr32.exe (interactive session)

UID: [redacted]

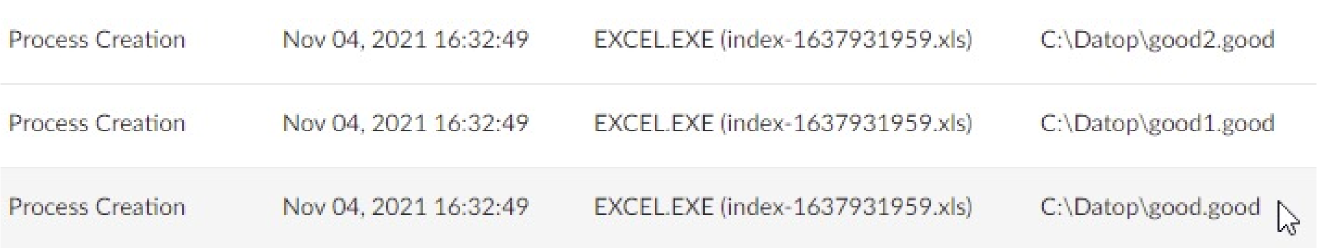
ID: 4328

Command Line: C:\Datop\good.good

Image Path: N/A

SHA1: N/A

Root: True



Process Creation	Nov 04, 2021 16:32:49	EXCEL.EXE (index-1637931959.xls)	C:\Datop\good2.good
Process Creation	Nov 04, 2021 16:32:49	EXCEL.EXE (index-1637931959.xls)	C:\Datop\good1.good
Process Creation	Nov 04, 2021 16:32:49	EXCEL.EXE (index-1637931959.xls)	C:\Datop\good.good

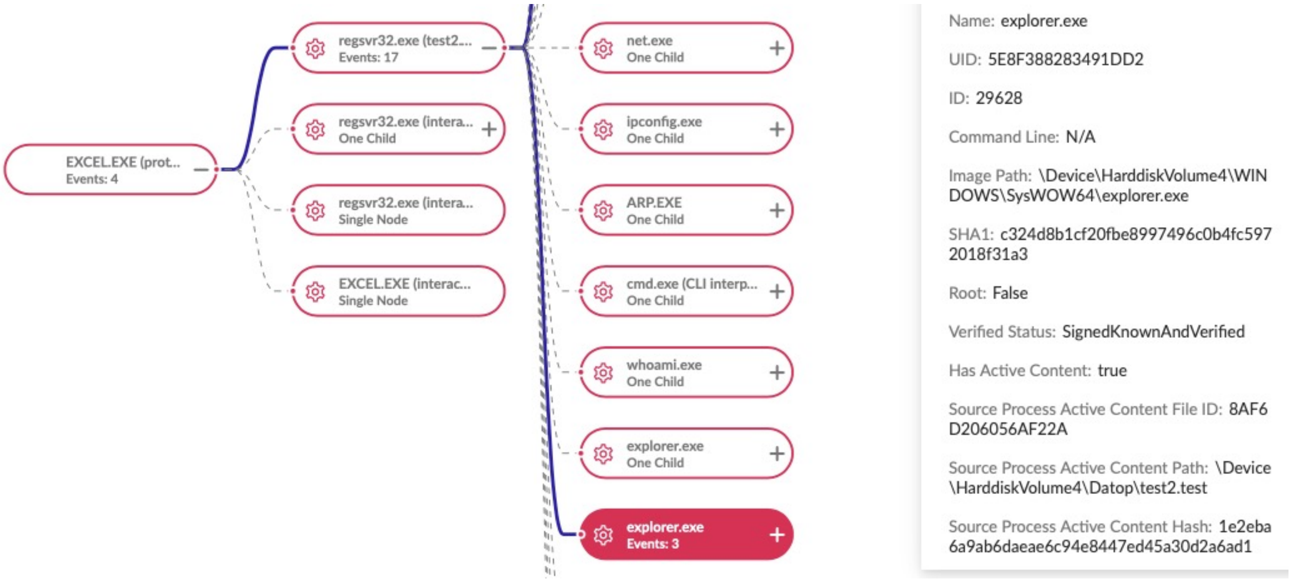
SquirrelWaffle Shares Code With Other Attack Frameworks

SquirrelWaffle, in common with many other malware samples, uses a custom crypter. Doing so is attractive for many reasons, not the least of which are obfuscation and anti-analysis to prevent researchers from developing strong indicators of compromise for detection.

Researchers have shown that SquirrelWaffle uses the same custom crypter as other well-known attack frameworks including Ursnif, Hancitor and Zloader. This is used, among other things, to hide the malware’s Command and Control (C2) URL.

Upon infection, SquirrelWaffle can download a Cobalt Strike payload with `.txt` extension and execute using the `WinExec` function. The other likely payload that may be downloaded by current SquirrelWaffle infections is Qakbot.

Below we can see process injection into `explorer.exe` from a SquirrelWaffle infection.



Name: explorer.exe

UID: 5E8F388283491DD2

ID: 29628

Command Line: N/A

Image Path: \Device\HarddiskVolume4\WINDOWS\SysWOW64\explorer.exe

SHA1: c324d8b1cf20fbe8997496c0b4fc5972018f31a3

Root: False

Verified Status: SignedKnownAndVerified

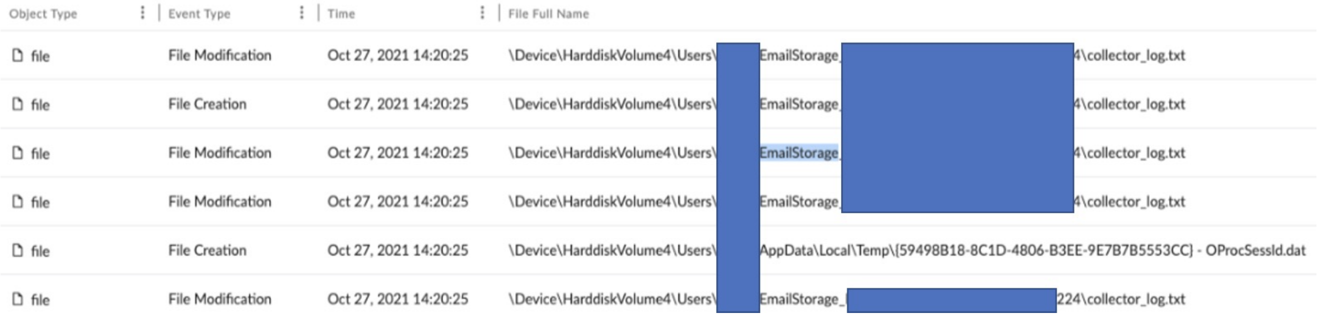
Has Active Content: true

Source Process Active Content File ID: 8AF6D206056AF22A

Source Process Active Content Path: \Device\HarddiskVolume4\Datop\test2.test

Source Process Active Content Hash: 1e2eba6a9ab6daeae6c94e8447ed45a30d2a6ad1

If infected with Qakbot, the malware will attempt to extract email data from the host.



Object Type	Event Type	Time	File Full Name
file	File Modification	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]EmailStorage_[redacted]4\collector_log.txt
file	File Creation	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]EmailStorage_[redacted]4\collector_log.txt
file	File Modification	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]EmailStorage_[redacted]4\collector_log.txt
file	File Modification	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]EmailStorage_[redacted]4\collector_log.txt
file	File Creation	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]AppData\Local\Temp\{59498B18-8C1D-4806-B3EE-9E7B7B5553CC} - OProcSessId.dat
file	File Modification	Oct 27, 2021 14:20:25	\Device\HarddiskVolume4\Users\[redacted]EmailStorage_[redacted]224\collector_log.txt

From the above image, we can see the `C:\Users\<user>\EmailStorage_<hostname>_<username>_<timestamp>` pattern. The “collector_log.txt” contains a record of the malware’s enumeration and exfiltration process.

How To Protect Against SquirrelWaffle

The SentinelOne platform detects and protects all customers against SquirrelWaffle infection. In the video demonstration below, we set the agent policy to ‘Detect Only’ to observe the infection in action. In ordinary circumstances, customers would use the Protect policy to prevent execution.

Watch Video At:

https://youtu.be/vdVfzu9M8G8

Conclusion

Cybercriminals are quick to come up with new loaders to team up with other groups that will help deliver a variety of payloads to achieve maximum financial gain. SquirrelWaffle is the latest such loader, currently being used to deliver Cobalt Strike and Qakbot but which can easily pivot to dropping any payload the operators wish. While SquirrelWaffle is certainly not yet anywhere near as prevalent as Emotet in its heyday, all the hallmarks are there of a campaign and infrastructure looking to grow.

If you would like to know more about how SentinelOne can protect your business against SquirrelWaffle and other threats, contact us for more information or request a free demo.

Example SHA1 Hashes

8d7089f17bd5706309d7c6986fdd1140d6c5b4b2
52452f6f0ab73531fe54935372d9c34eb50653d8
bce0e9e1c6d2e7b12648ef316748191f10ed8582
8ba7694017d1cea1d4b73f39479726478df88b20
8aec96029b83d3b226c8c83dd90f48946ee97001
8262cd7029f943a7b6199b5a6c51ec19e085c3b7