SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

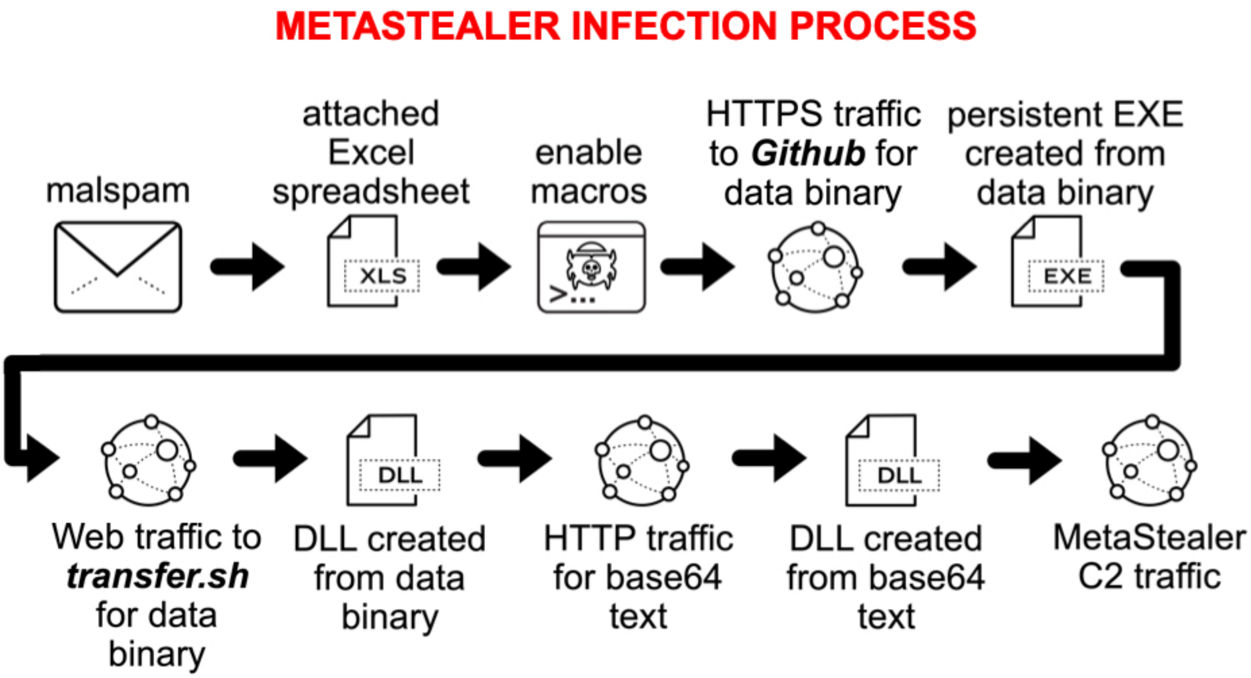
isc.sans.edu/diary/rss/28522

Windows MetaStealer Malware

Published: 2022-04-06
Last Updated: 2022-04-06 03:50:00 UTC
by Brad Duncan (Version: 1)
0 comment(s)

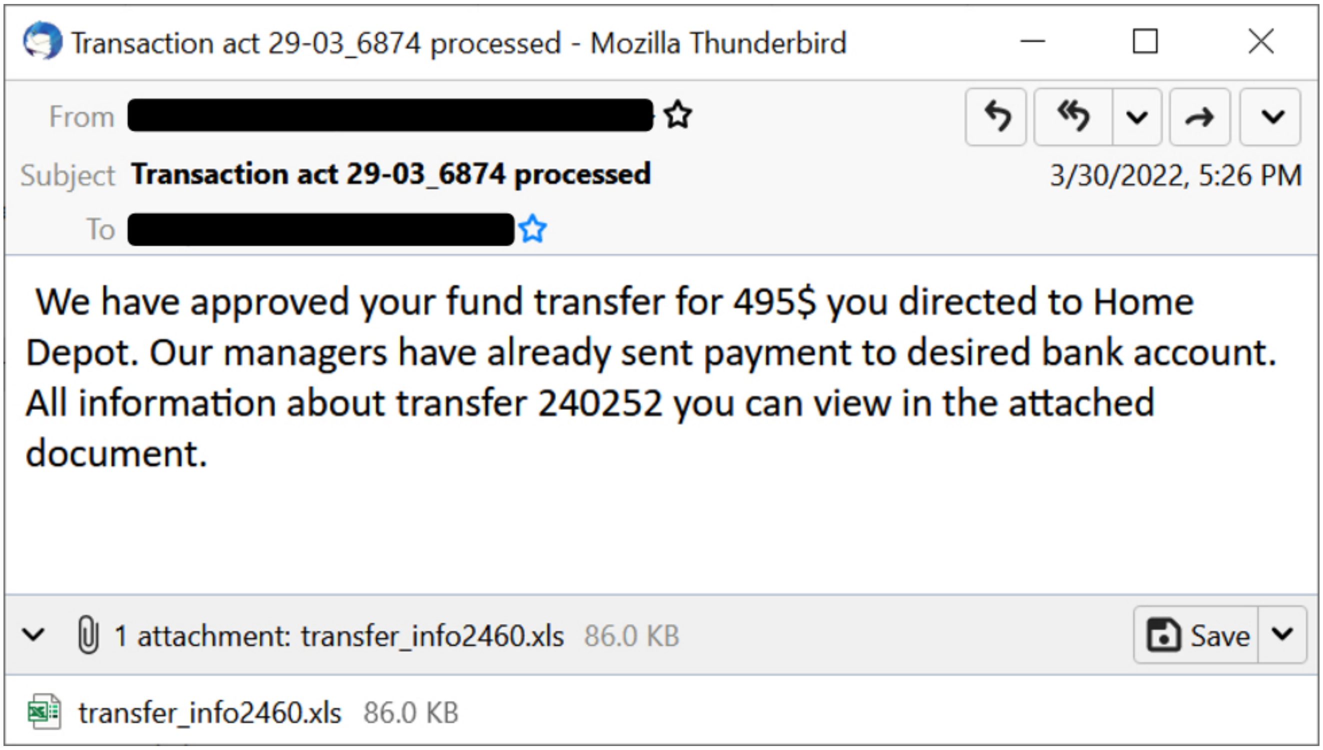
Introduction

- Since Wednesday 2022-03-30, at least 16 samples of a specific Excel file have been submitted to VirusTotal.
- These malicious Excel files are distributed as email attachments.
- Post-infection traffic triggers signatures for ***Win32/MetaStealer Related Activity*** from the EmergingThreats Pro (ETPRO) ruleset.
- This infection process uses data binaries to create the malicious EXE and DLL files used for the infection.
- The malware abuses legitimate services by Github and transfer.sh to host these data binaries.
- All URLs, domains, and IP addresses were still active for the infection approximately 3 hours before I posted this diary.


METASTEALER INFECTION PROCESS
malspam
attached Excel spreadsheet
XLS
enable macros
>...
HTTPS traffic to ***Github*** for data binary
persistent EXE created from data binary
EXE
Web traffic to ***transfer.sh*** for data binary
DLL created from data binary
DLL
HTTP traffic for base64 text
DLL created from base64 text
DLL
MetaStealer C2 traffic

Shown above: Flow chart for the MetaStealer infection chain reviewed in today's diary.

Images from an infection



From [redacted]

Subject **Transaction act 29-03_6874 processed** 3/30/2022, 5:26 PM

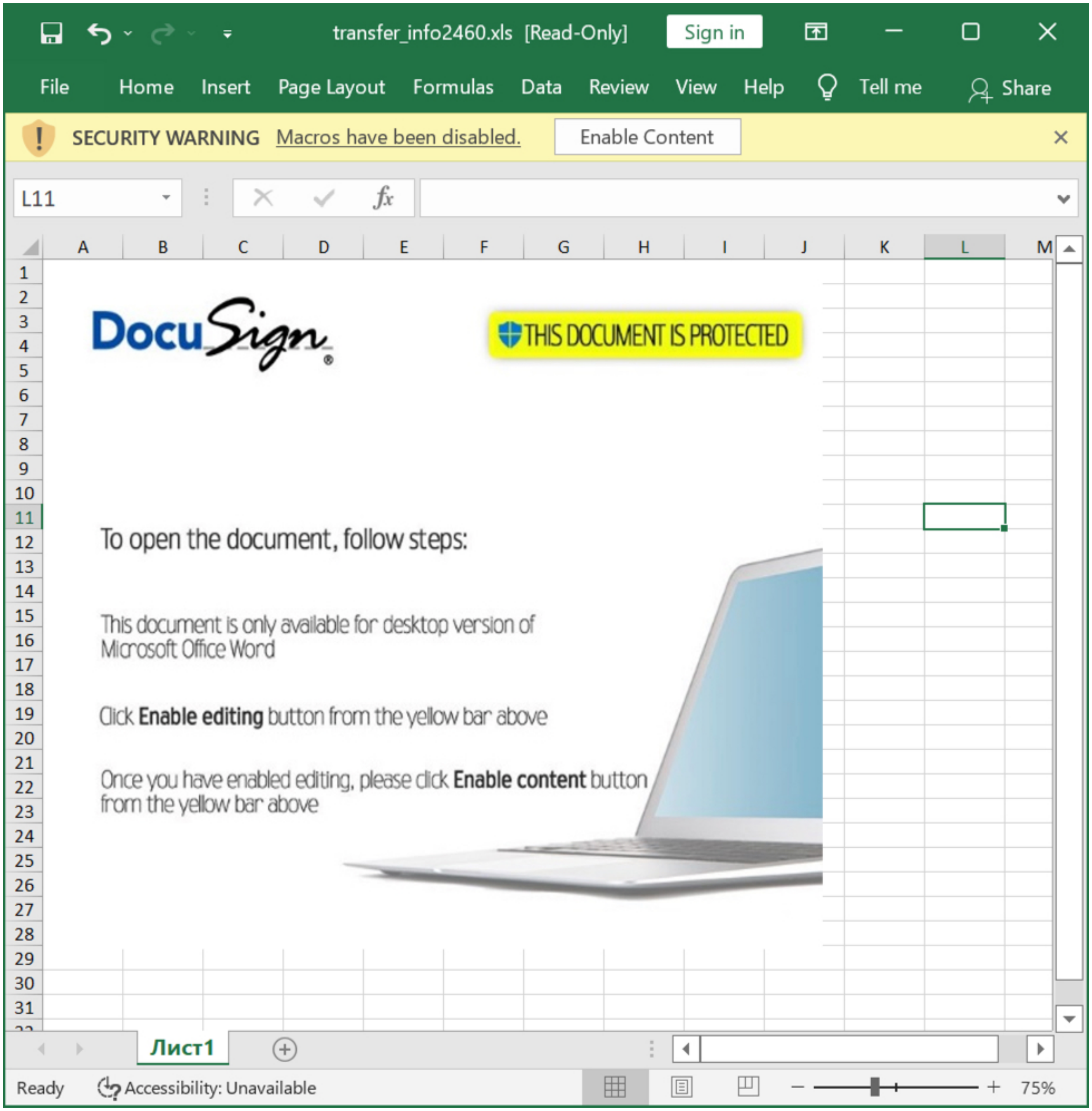
To [redacted]

We have approved your fund transfer for 495$ you directed to Home Depot. Our managers have already sent payment to desired bank account. All information about transfer 240252 you can view in the attached document.

1 attachment: transfer_info2460.xls 86.0 KB

transfer_info2460.xls 86.0 KB

Shown above: Screenshot from an email distributing the malicious Excel file.



SECURITY WARNING Macros have been disabled. Enable Content

THIS DOCUMENT IS PROTECTED

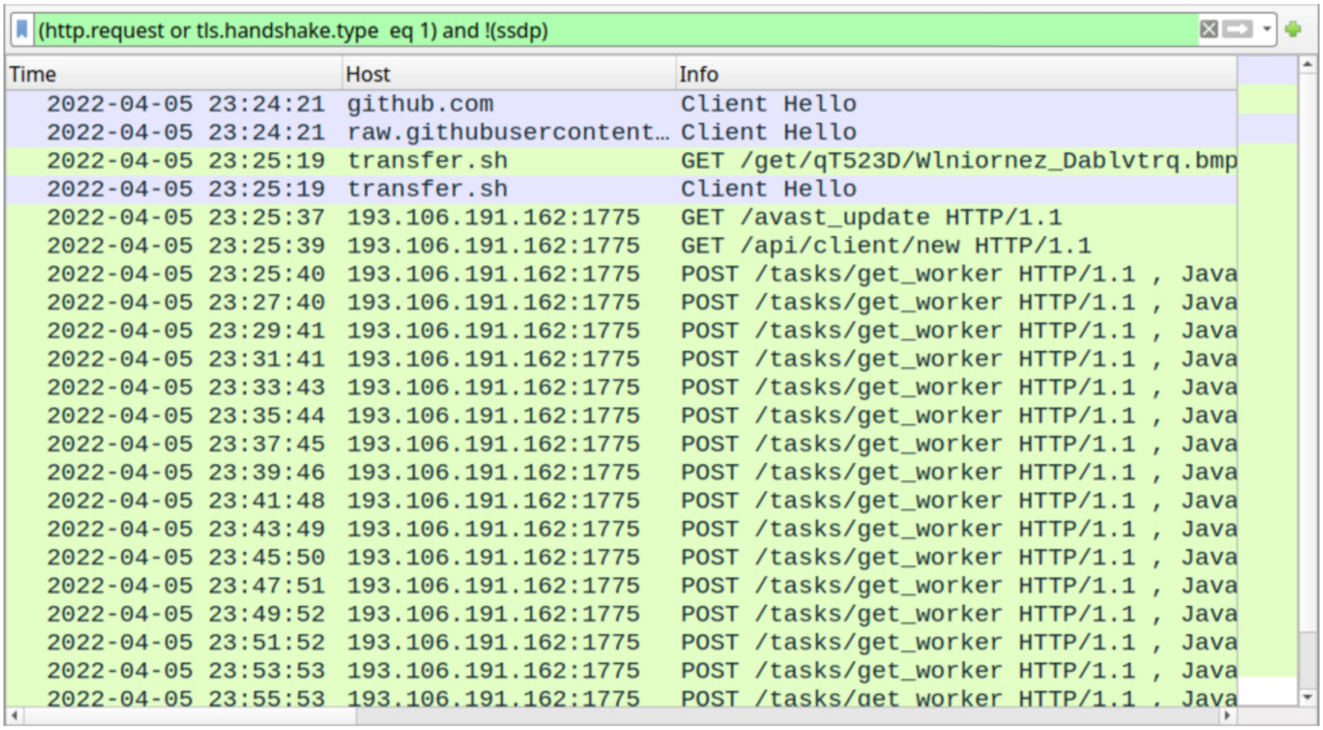
To open the document, follow steps:

This document is only available for desktop version of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

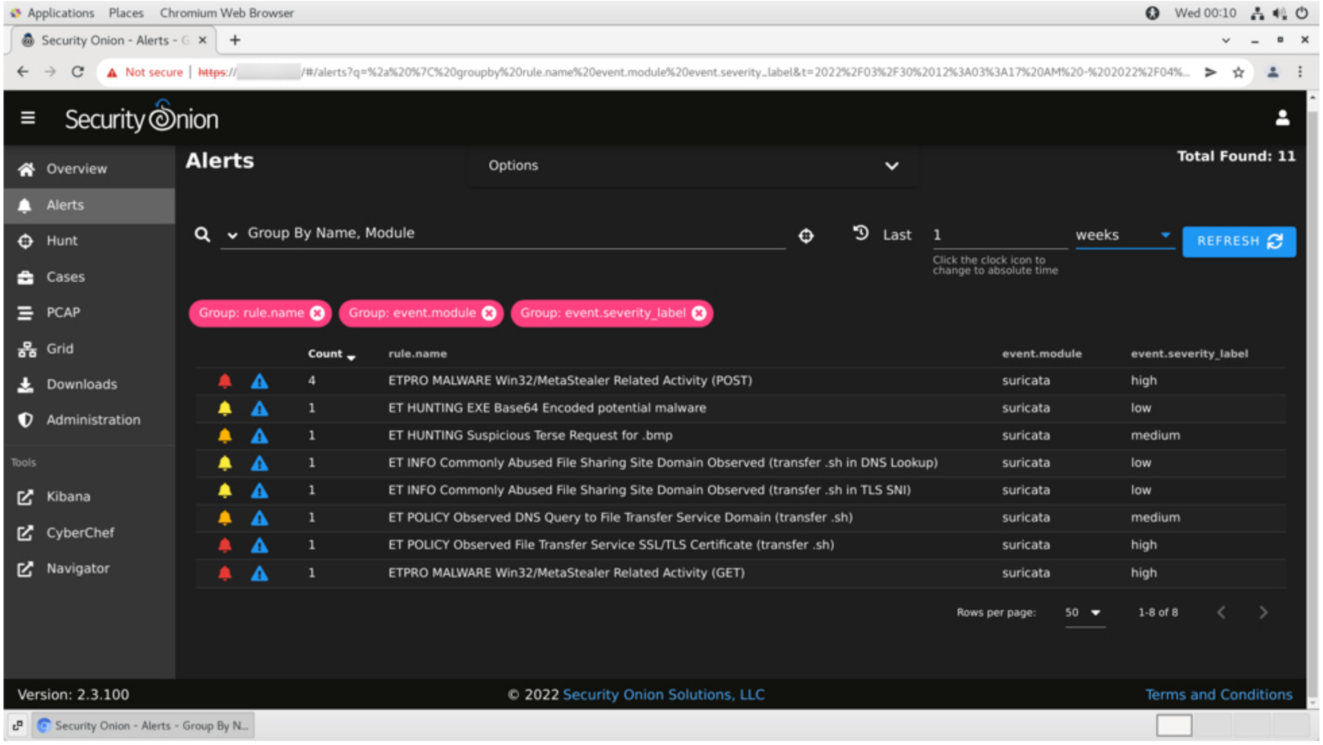
Shown above: Screenshot of the malicious Excel file.



```
(http.request or tls.handshake.type  eq 1) and !(ssdp)

Time                  Host                       Info
 2022-04-05 23:24:21  github.com                 Client Hello
 2022-04-05 23:24:21  raw.githubusercontent…     Client Hello
 2022-04-05 23:25:19  transfer.sh                GET /get/qT523D/Wlniornez_Dablvtrq.bmp
 2022-04-05 23:25:19  transfer.sh                Client Hello
 2022-04-05 23:25:37  193.106.191.162:1775       GET /avast_update HTTP/1.1
 2022-04-05 23:25:39  193.106.191.162:1775       GET /api/client/new HTTP/1.1
 2022-04-05 23:25:40  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:27:40  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:29:41  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:31:41  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:33:43  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:35:44  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:37:45  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:39:46  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:41:48  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:43:49  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:45:50  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:47:51  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:49:52  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:51:52  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:53:53  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
 2022-04-05 23:55:53  193.106.191.162:1775       POST /tasks/get_worker HTTP/1.1 , Java
```

Shown above: Traffic from an infection on Tuesday 2022-04-05 filtered in Wireshark.



https://[redacted]/#/alerts?q=%2a%20%7C%20groupby%20rule.name%20event.module%20event.severity_label&t=2022%2F03%2F30%2012%3A03%3A17%20AM%20-%202022%2F04%...

Alerts

Total Found: 11

Group By Name, Module

Last 1 weeks

Click the clock icon to change to absolute time

Group: rule.name · Group: event.module · Group: event.severity_label

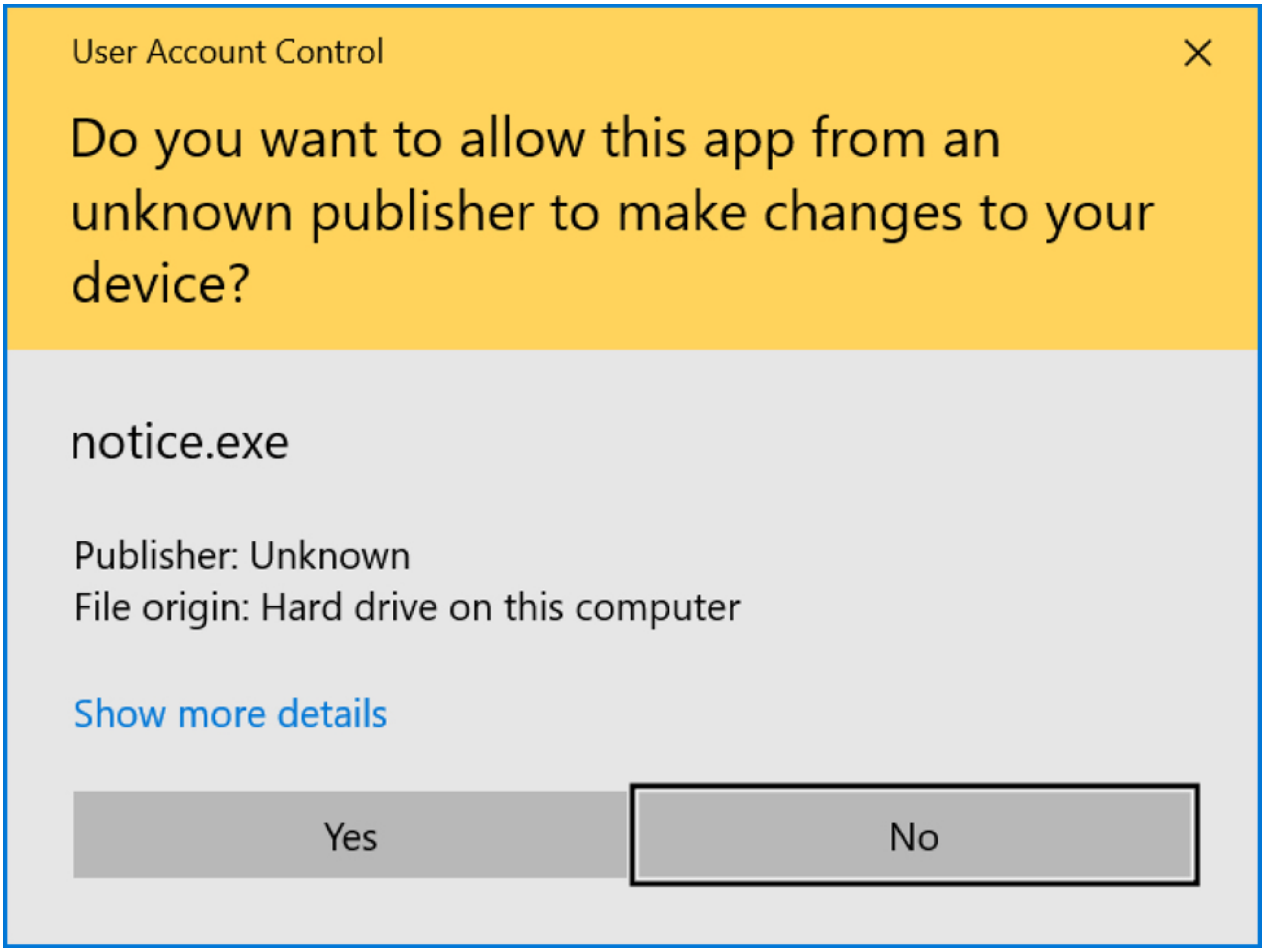
		Count	rule.name	event.module	event.severity_label
🔔	⚠	4	ETPRO MALWARE Win32/MetaStealer Related Activity (POST)	suricata	high
🔔	⚠	1	ET HUNTING EXE Base64 Encoded potential malware	suricata	low
🔔	⚠	1	ET HUNTING Suspicious Terse Request for .bmp	suricata	medium
🔔	⚠	1	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)	suricata	low
🔔	⚠	1	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)	suricata	low
🔔	⚠	1	ET POLICY Observed DNS Query to File Transfer Service Domain (transfer .sh)	suricata	medium
🔔	⚠	1	ET POLICY Observed File Transfer Service SSL/TLS Certificate (transfer .sh)	suricata	high
🔔	⚠	1	ETPRO MALWARE Win32/MetaStealer Related Activity (GET)	suricata	high

Rows per page: 50 1-8 of 8

Version: 2.3.100

© 2022 Security Onion Solutions, LLC

Shown above: Alerts from the infection Security Onion using the Suricata and the ETPRO ruleset.



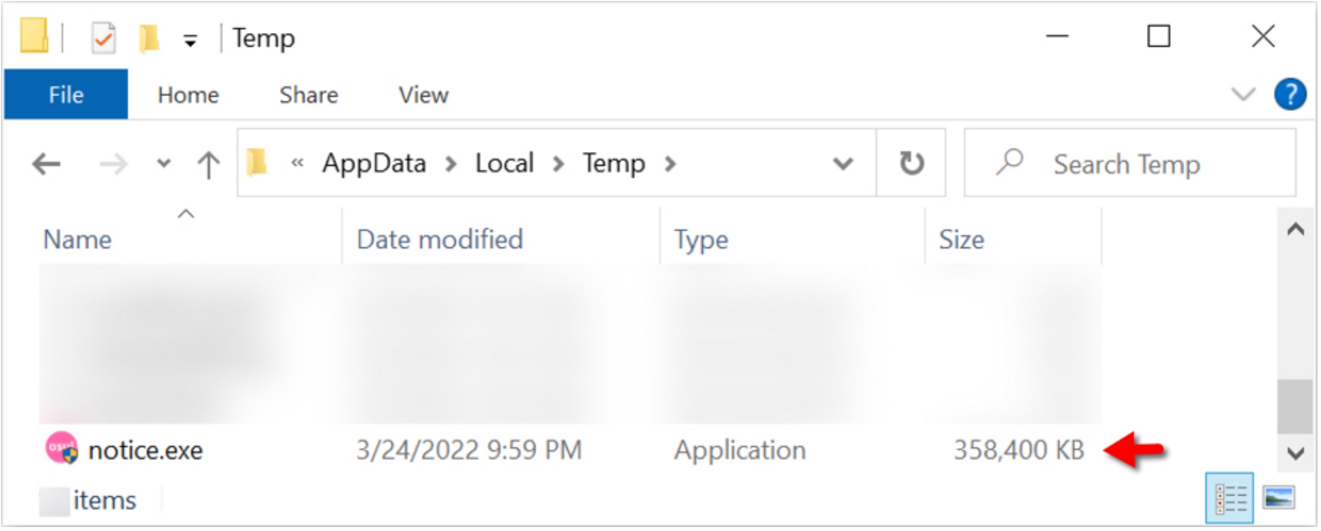
User Account Control

Do you want to allow this app from an unknown publisher to make changes to your device?

notice.exe

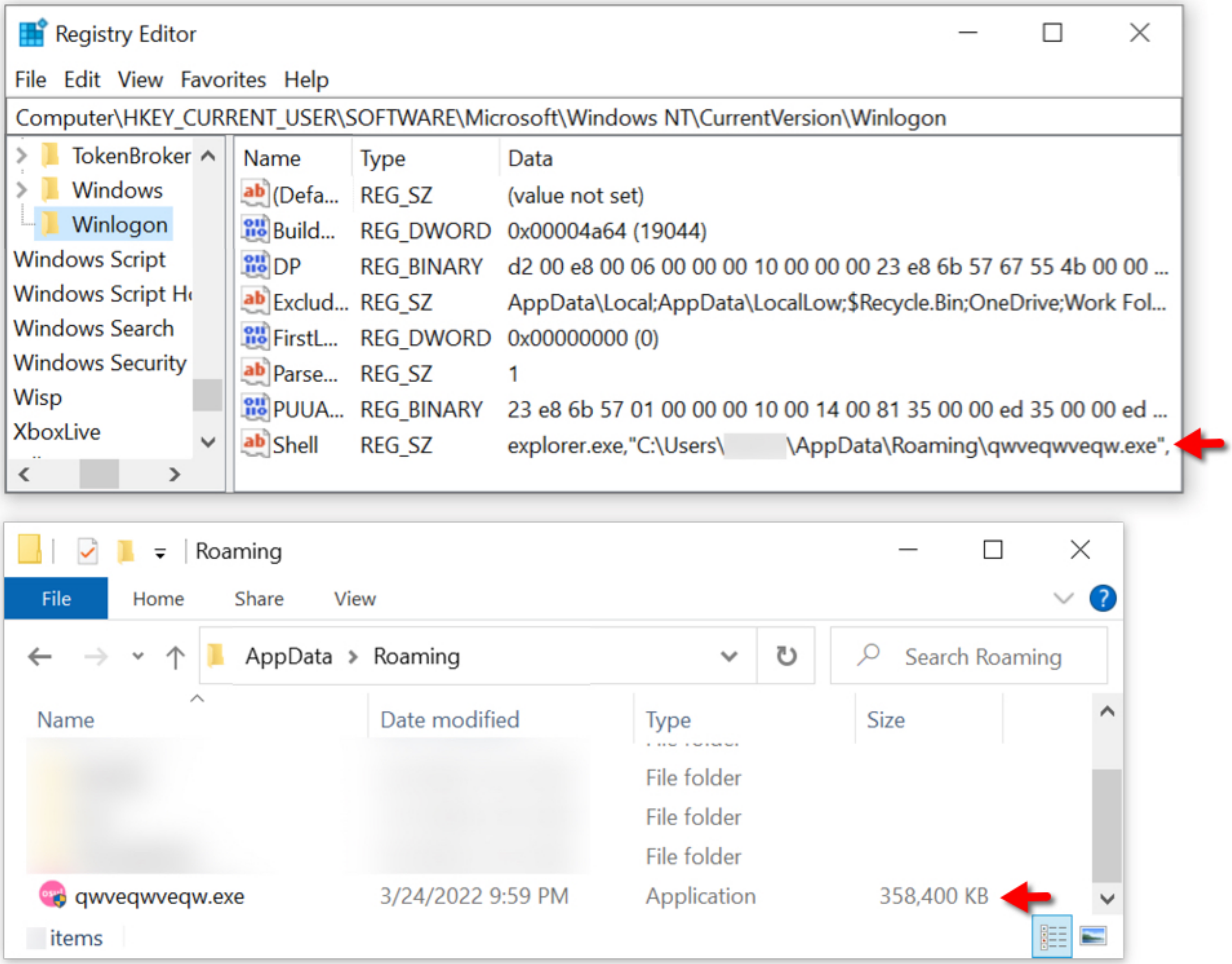
Publisher: Unknown
File origin: Hard drive on this computer

Shown above: UAC alert generated by malicious EXE during the infection.



Name	Date modified	Type	Size
notice.exe	3/24/2022 9:59 PM	Application	358,400 KB

Shown above: Malicious EXE file generated during the infection.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Name	Type	Data
(Defa...	REG_SZ	(value not set)
Build...	REG_DWORD	0x00004a64 (19044)
DP	REG_BINARY	d2 00 e8 00 06 00 00 00 10 00 00 00 23 e8 6b 57 67 55 4b 00 00 ...
Exclud...	REG_SZ	AppData\Local;AppData\LocalLow;$Recycle.Bin;OneDrive;Work Fol...
FirstL...	REG_DWORD	0x00000000 (0)
Parse...	REG_SZ	1
PUUA...	REG_BINARY	23 e8 6b 57 01 00 00 00 10 00 14 00 81 35 00 00 ed 35 00 00 ed ...
Shell	REG_SZ	explorer.exe,"C:\Users\[redacted]\AppData\Roaming\qwveqwveqw.exe",

Name	Date modified	Type	Size
[redacted]	[redacted]	File folder	
		File folder	
		File folder	
qwveqwveqw.exe	3/24/2022 9:59 PM	Application	358,400 KB

[redacted] items

Shown above: Malicious EXE persistent on the infected Windows host.

Indicators of Compromise (IOCs)

Traffic generated after enabling Excel macro:

- hxxps://github[.]com/michel15P/1/raw/main/notice.zip
- hxxps://raw.githubusercontent[.]com/michel15P/1/main/notice.zip
- Note: File returned from the above URL is a data binary and not a zip archive

Traffic generated by persistent EXE created from the above binary:

- port 80 - transfer[.]sh - GET /get/qT523D/Wlniornez_Dablvtrq.bmp
- port 443 - hxxps://transfer[.]sh/get/qT523D/Wlniornez_Dablvtrq.bmp

- 193.106.191[.]162 port 1775 - 193.106.191[.]162:1775 - GET /avast_update
- 193.106.191[.]162 port 1775 - 193.106.191[.]162:1775 - GET /api/client/new

- 193.106.191[.]162 port 1775 - 193.106.191[.]162:1775 - POST /tasks/get_worker

Alerts on traffic to 193.106.191[.]162 over TCP port 1775:

- ETPRO MALWARE Win32/MetaStealer Related Activity (GET) sid: 2851362
- ETPRO MALWARE Win32/MetaStealer Related Activity (POST) sid: 2851363

Associated malware and artifacts:

SHA256 hash:
981247f5f23421e9ed736dd462801919fea2b60594a6ca0b6400ded463723a5e

- File size: 88,069 bytes
- File name: transfer_info2460.xls
- File description: Example of email attachment, an Excel file with macro for malware
- Sandbox analysis: https://app.any.run/tasks/02a6b252-5ea1-4f2b-96d3-4eb2eaec34ca

SHA256 hash: 81e77fb911c38ae18c268178492224fab7855dd6f78728ffedfff6b62d1279dc

- File size: 2,828 bytes
- File name: open.vbs
- File location: same directory as the above Excel file or the user's AppData/Local/Temp directory
- File description: After enabling macro, this VBS file is used to create the persistent EXE
- Note: I could not find this file on my infected lab host

SHA256 hash:
8cfa23b5f47ee072d894ee98b1522e3b8acc84a6e9654b71f50536e74a3579a5

- File size: 417,512 bytes
- File location: hxxps://raw.githubusercontent[.]com/michel15P/1/main/notice.zip
- File type: data
- File description: data binary retrieved by open.vbs used to persistent EXE (below)

SHA256 hash: f644bef519fc0243633d13f18c97c96d76b95b6f2cbad2a2507fb8177b7e4d1d

- File size: 367,001,600 bytes
- File location: C:\Users\*[username]*\AppData\Local\Temp\notice.exe
- File location: C:\Users\*[username]*\AppData\Roaming\qwveqwveqw.exe
- File description: Malware EXE persistent on the infected Windows host
- Note: This binary is appended with more than 366 MB of zero byte filler
- Note: Persistent through "Shell" value at HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

SHA256 hash:
7641ae596b53c5de724101bd6df35c999c9616d93503bce0ffd30b1c0d041e3b

- File size: 143,400 bytes
- File description: Persistent malware EXE with most of the zero byte filler removed

SHA256 hash:
fba945b78715297f922b585445c74a4d7663ea2436b8c32bcb0f4e24324d3b8b

- File size: 716,288 bytes
- File location: hxxps://transfer[.]sh/get/qT523D/Wlniornez_Dablvtrq.bmp
- File type: data
- File description: Retrieved by persistent EXE, this binary is a Windows DLL file in reverse byte order

SHA256 hash: bf3b78329eccd049e04e248dd82417ce9a2bcaca021cda858affd04e513abe87

- File size: 716,288 bytes
- File description: Windows DLL file created by reserving the above binary
- File type: PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
- Run method: loaded/run by persistent EXE

SHA256 hash:
cb6254808d1685977499a75ed2c0f18b44d15720c480fb407035f3804016ed89

- File size: 2,182,488 bytes
- File location: hxxp://193.106.191[.]162:1775/avast_update
- File description: base64 text representing a Windows DLL file

SHA256 hash:
71e54b829631b93adc102824a4d3f99c804581ead8058b684df25f1c9039b738

- File size: 1,636,864 bytes
- File description: Windows DLL file converted from the above text
- File type: PE32 executable (DLL) (console) Intel 80386, for MS Windows
- Run method: unknown, loaded/run by persistent EXE or previous DLL loaded/run by persistent EXE

Final words

Each time I rebooted my infected Windows host, the persistent EXE generated traffic to the same ***transfer.sh*** URL and re-started the infection process without the Github traffic.

Malware associated with this infection was first submitted to VT on Wednesday 2022-03-30. ETPRO signatures identifying HTTP traffic generated by this malware as MetaStealer were released on Friday 2022-04-01.

My thanks to Security Onion, Proofpoint's EmergingThreats team, and Didier Stevens' tools for reversing binaries. These three resources were a big help in my analysis for this diary.

A pcap of the infection traffic and the associated malware/artifacts can be found here.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: DLL Excel EXE Malspam Malware MetaStealer Windows

0 comment(s)

DEV522 Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked

Top of page

×

Diary Archives