

# Windows MetaStealer Malware - SANS Internet Storm Center

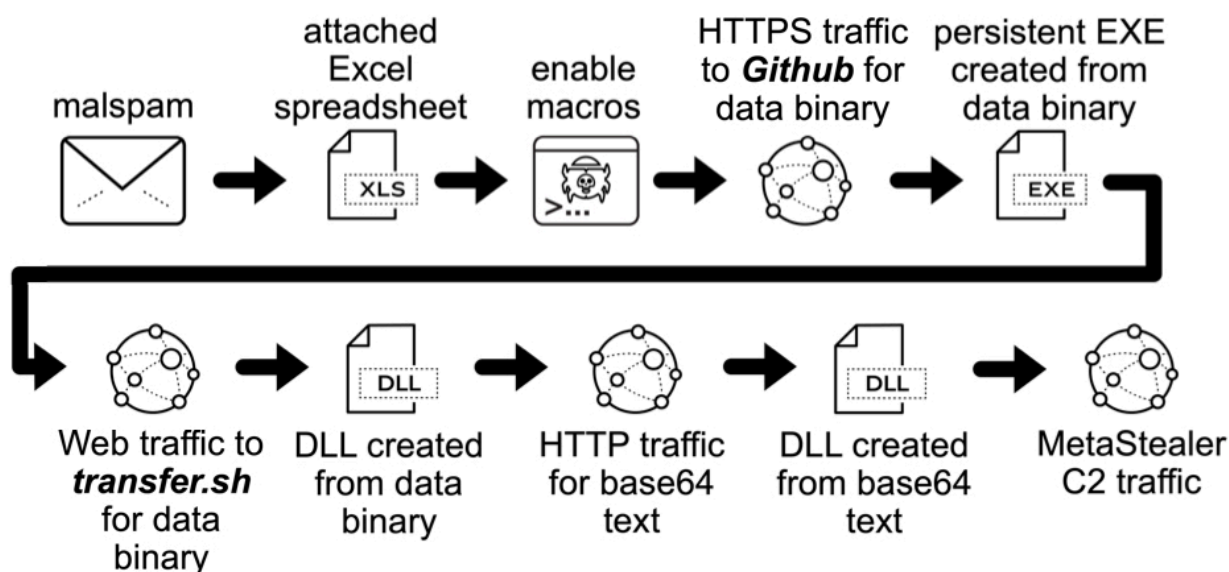
By SANS Internet Storm Center

Archived: 2026-04-05 17:41:16 UTC

## 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



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

## Images from an infection

Transaction act 29-03\_6874 processed - Mozilla Thunderbird

From [REDACTED] ☆

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

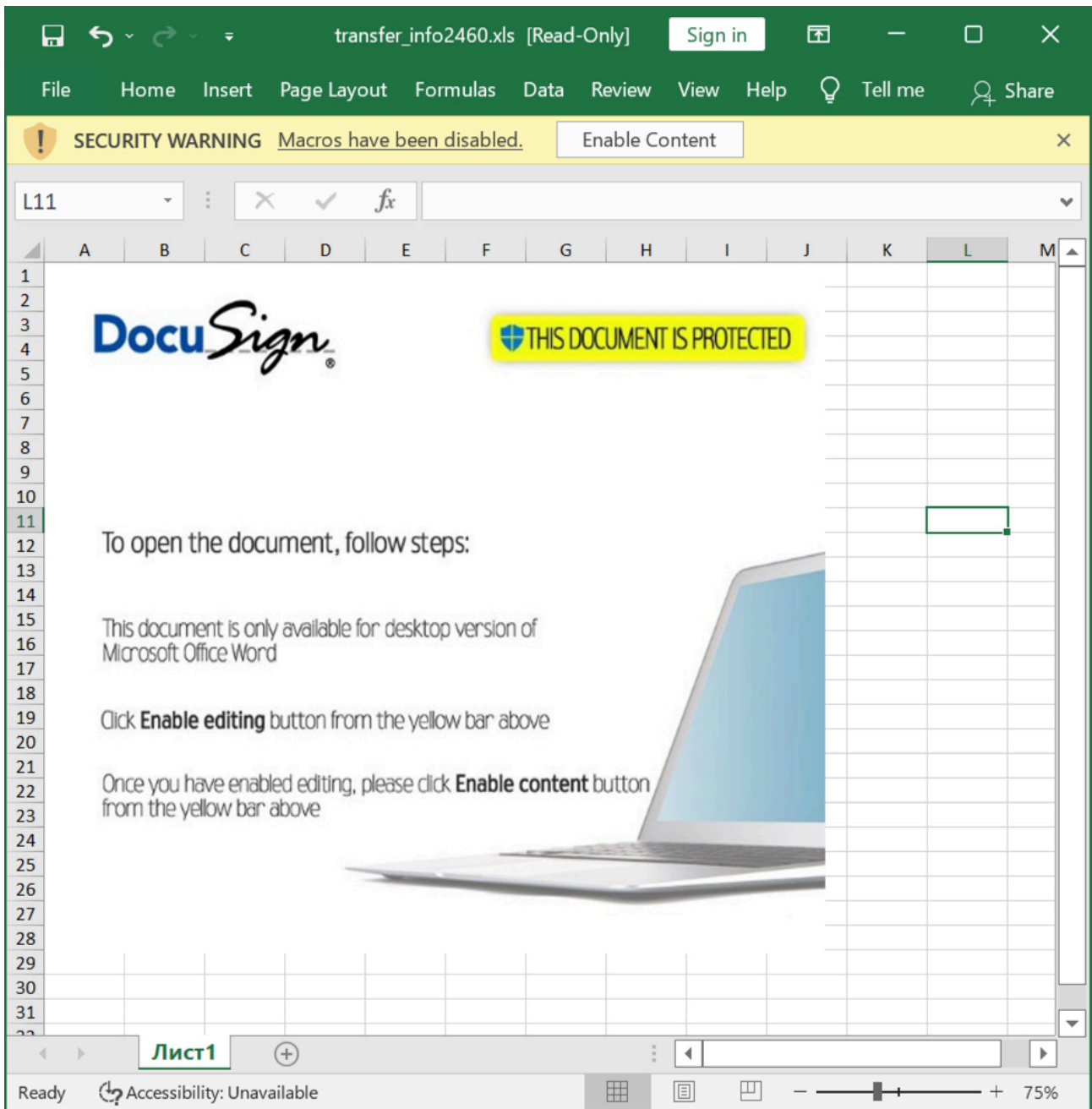
To [REDACTED] ☆

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.



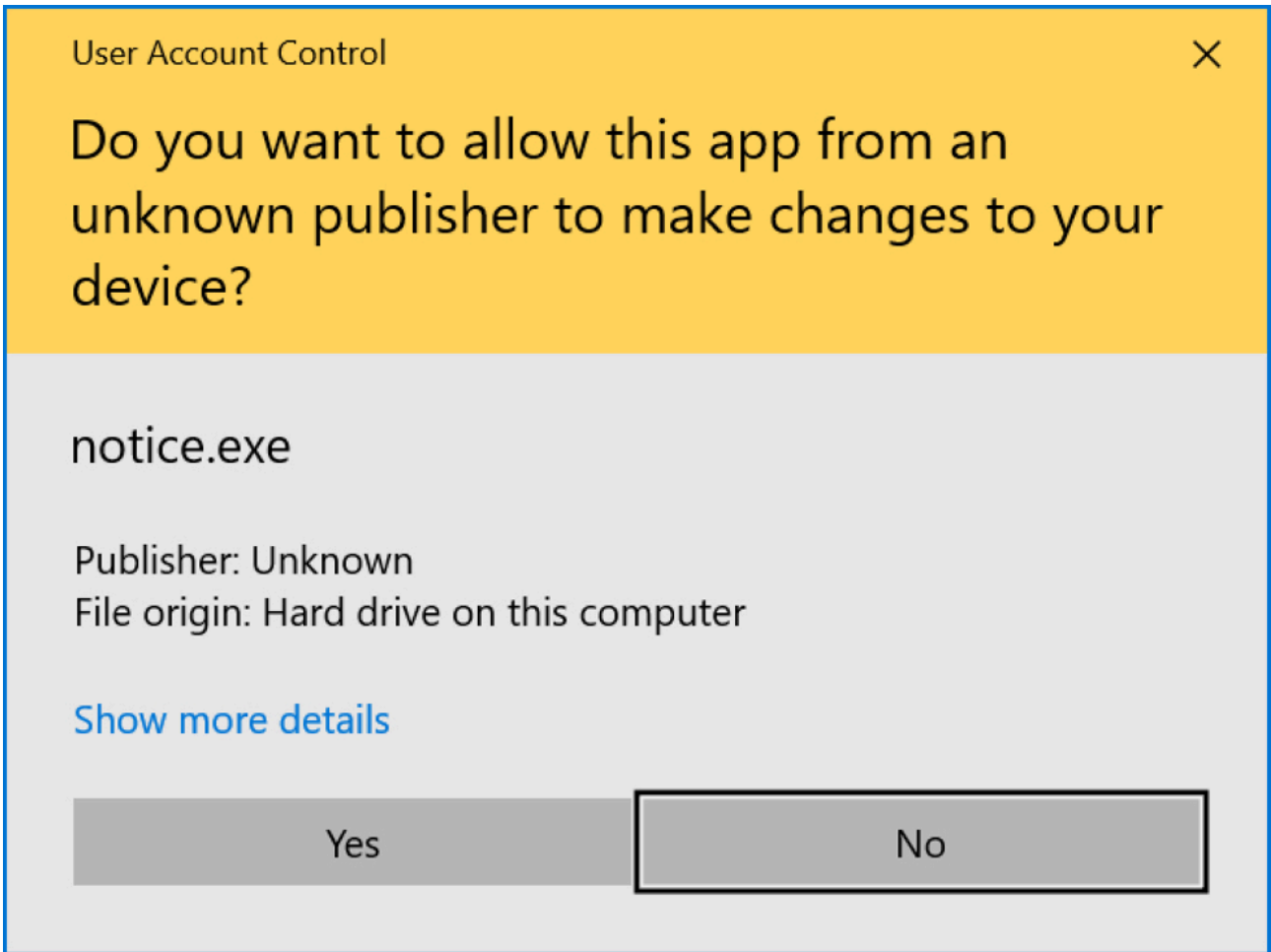
Shown above: Screenshot of the malicious Excel file.

Time	Host	Info
2022-04-05 23:24:21	github.com	Client Hello
2022-04-05 23:24:21	raw.githubusercontent.com	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

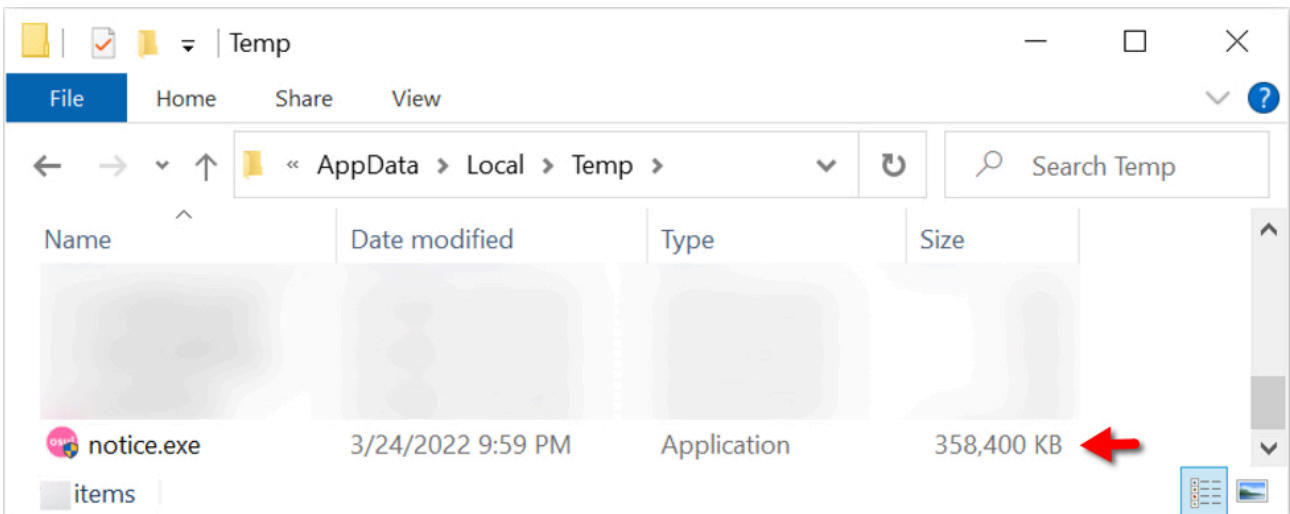
Shown above: Traffic from an infection on Tuesday 2022-04-05 filtered in Wireshark.

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

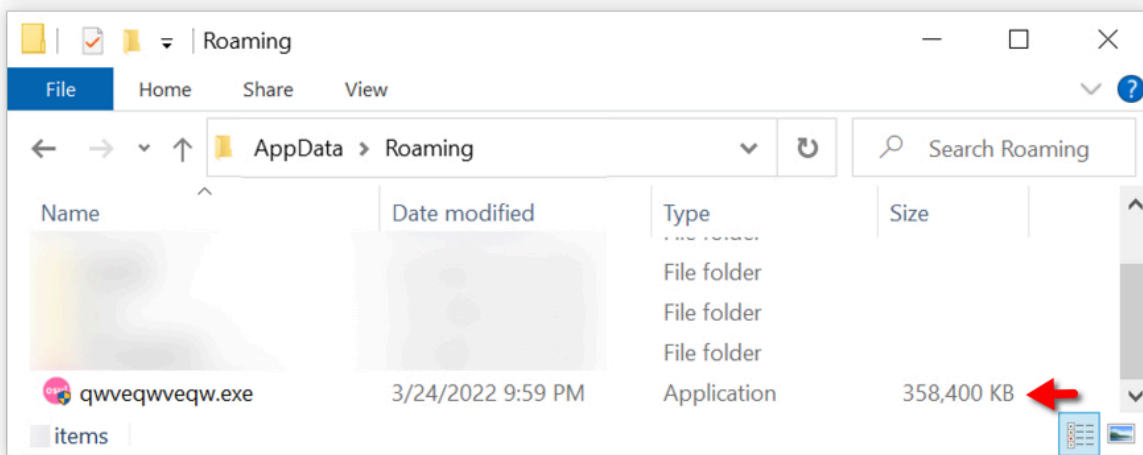
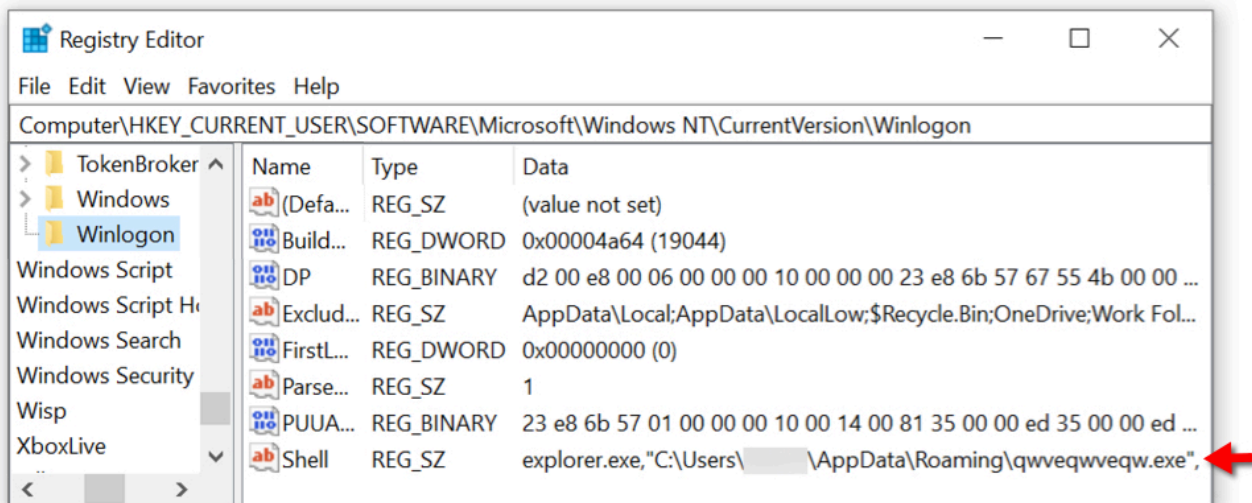
Shown above: Alerts from the infection Security Onion using the Suricata and the ETPRO ruleset.



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



Shown above: Malicious EXE file generated during the infection.



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](https://github.com/michel15P/1/raw/main/notice.zip)
- [hxxps://raw.githubusercontent.com/michel15P/1/main/notice.zip](https://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](https://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

---

Source: <https://isc.sans.edu/forums/diary/Windows+MetaStealer+Malware/28522/>