

UBNETDEF Network Activity Report

Date: 2023-04-17

EXECUTIVE SUMMARY

On April 17, 2023, a Windows host with IP address 172.16.0.149 was infected with the Dridex trojan. The malware spread to other devices within the organization, specifically targeting 172.16.0.170 and 172.16.0.131. This infection poses a significant threat to network security, as Dridex is known for stealing sensitive information and exploiting vulnerabilities. To resolve this issue, it is crucial to remove the malware, implement stricter security measures, and prevent future infections.

CONTENTS

Executive Summary 1

Technical Analysis 2-5

Recommended Clean-Up and Mitigation Strategies 6

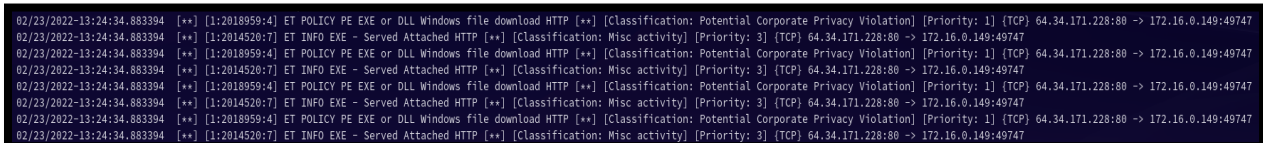
Contributing Analysts 7

TECHNICAL ANALYSIS

The Suricata IDS/IPS alerts indicated that the initial Dridex infection involved a file download from a malicious domain, "www.ajaxmatters.com". The file was named "2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll" and was downloaded onto the machine with IP address 172.16.0.149. Further investigation revealed connections to other malicious IP addresses:

135.148.121.246, 27.254.174.84, 64.34.171.228, 23.227.38.74, 198.54.117.215.

All of the malicious IPs are reported on virus total which is a reporting webpage. The bad actor used the Dridex trojan and the malicious IP's to spread to devices 172.16.0.170 and 172.16.0.131 within the organization's internal network.



```
02/23/2022-13:24:34.883394 [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2014520:7] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2014520:7] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2014520:7] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
02/23/2022-13:24:34.883394 [**] [1:2014520:7] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] (TCP) 64.34.171.228:80 -> 172.16.0.149:49747
```

Figure 1

The Machine 172.16.0.149 downloads an executable file from 64.34.171.228. This file triggered a Corporate Privacy Violation.



Figure 2

Machine 172.16.0.149 downloads the file

"2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll" from www.ajaxmatters.com

allowing the Dridex Trojan in.

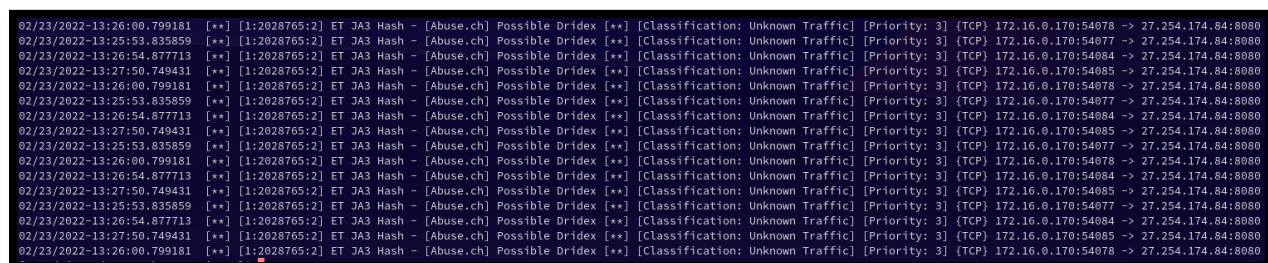


Figure 3

The malware spreads inside the network. Communication between

172.16.0.170 and 27.254.174.84.

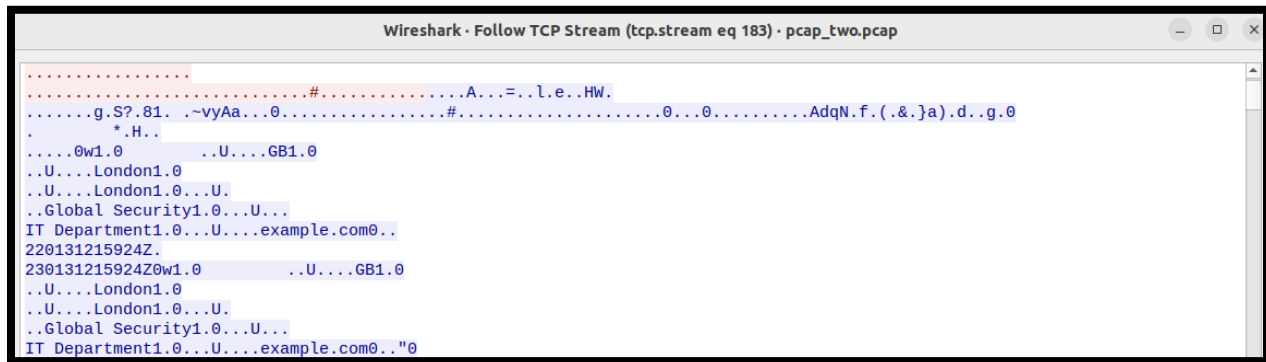


Figure 4

Inside 27.254.174.84 and 172.16.0.170 communication.



Figure 5

Suricata detection on communication between 172.16.0.131 and 216.172.184.77. Suricata detected this classification as "Malware Command and Control Activity"

```
Wireshark · Follow TCP Stream (tcp.stream eq 272) · pcap_two.pcap
GET /uar3/?WN68=wLPqDi6WkwhBj433Ws1QWRAisb43Y4vnWD77yX4A6l/EM3iK/pFUTvPwCnDSQCKQYsapKIpket25I1F4noK8Q==&OxtD9L=cFNTMFx8k4S1
HTTP/1.1
Host: www.db-propertygroup.com
Connection: close

.....HTTP/1.1 403 Forbidden
Date: Wed, 23 Feb 2022 18:33:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
X-Sorting-Hat-PodId: 199
X-Sorting-Hat-ShopId: 59896299720
X-Dc: gcp-us-central1
X-Request-ID: 3e1ad5a2-1477-4218-931b-bd92cc002c13
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
CF-Cache-Status: DYNAMIC
Server: cloudflare
CF-RAY: 6e228a46c93eccc3-DFW
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

141d
```

Figure 6

Evidence 172.16.0.131 has communicated with a bad actor.

6
/ 89

Community Score

6 security vendors flagged this URL as malicious

http://www.db-propertygroup.com/
www.db-propertygroup.com

403
Status

2022-10-04 19:43:40 UTC
7 months ago

DETECTION

DETAILS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Do you want to automate checks?

BitDefender	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-DATA	Malware
Sophos	Malware	Webroot	Malicious

Figure 7

Total virus report for www.db-propertygroup.com. This site is flagged for malware.

RECOMMENDED CLEAN UP AND MITIGATION STRATEGIES

First, isolate the affected machines on the network (172.16.0.149, 172.16.0.170, and 172.16.0.131) by powering them down. Additionally, disconnect them from the network to prevent further infection or data exfiltration. Then remove the Dridex malware from the infected hosts by identifying and deleting associated files, such as the file "2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll", and any registry entries. Update antivirus software and ensure that it scans for Dridex trojan signatures. Implement strict firewall rules to block connections to known malicious domains and IP addresses associated with the Dridex trojan. Monitor network traffic for unusual patterns or connections, particularly those involving the malicious IP addresses identified. Educate users on safe browsing practices and the importance of not clicking on suspicious links or downloading unknown files. By following these steps, the infected hosts can be cleaned, and future infections can be prevented.

CONTRIBUTING ANALYSTS

Lead Analyst: Joshua Crull