

WARZONE 1 - TIER 1 SECURITY ANALYST L1 - MSSP (MANAGED SECURITY SERVICE PROVIDER) - PRE-REPORT NOTES - BRIM | NETWORKMINER | WIRESHARK

INFORMATION:

IDS/IPS ALERTS WHERE RECEIVED: POTENTIALLY BAD TRAFFIC & MALWARE COMMAND & CONTROL ACTIVITY DETECTED. SOC 1 ANALYST: TRIAGE.

SCOPE:

THE INVESTIGATION FOCUSED ON IDS/IPS ALERTS FLAGGED AS POTENTIALLY MALICIOUS TRAFFIC AND COMMAND-AND-CONTROL (C2) ACTIVITY. THE PRIMARY DATA SOURCE WAS A PCAP FILE NAMED ZONE1.PCAP, WHICH CONTAINED A TOTAL OF 1,808 NETWORK FLOWS RECORDED ON OCTOBER 5TH, 2021. ANALYSIS WAS CONDUCTED USING BRIM, NETWORKMINER, AND WIRESHARK TO IDENTIFY SUSPICIOUS CONNECTIONS, MALWARE ARTIFACTS, AND ASSOCIATED ADVERSARY INFRASTRUCTURE. THE SCOPE WAS LIMITED TO TRAFFIC PRESENT IN THE PCAP FILE AND DID NOT INCLUDE HOST-BASED FORENSICS OR ENDPOINT TELEMETRY.

INVESTIGATION:

-THE SIGNATURE DETECTED FROM THE MALWARE COMMAND & CONTROL ACTIVITY WAS: "ET MALWARE MIRRORBLAST CNC ACTIVITY M3". SOURCE IP ADDRESS 172[.]16[.]1[.]102 PORT: 53269. DESTINATION IP ADDRESS 169[.]239[.]128[.]11 PORT: 80 ON 10/05/2021 @ 22:43:17.787. THE DESTINATION IP ADDRESS IS ASSOCIATED WITH A COMPANY CALLED 'ZAPPIE HOST LLC'. ZAPPIE HOST IS A BUSINESS GRADE LINUX & WINDOWS SSD VPS SERVER PROVIDER. ZAPPIE IS LOCATED IN NEW ZEALAND BUT THE IP ADDRESS 169[.]239[.]128[.]11 IS ORIGINATING FROM SOUTH AFRICA (ZA) ACCORDING TO VIRUS TOTAL.

2021-10-05T22:43:17.787	alert	172.16.1.102	53269	169.239.128.11	80	TCP	http	1	ET MALWARE MirrorBlast CnC Activity M3	Malware Command and
2021-10-05T22:43:17.787	alert	172.16.1.102	53269	169.239.128.11	80	TCP	http	2	ET USER_AGENTS Suspicious User-Agent (REBOL)	Potentially Ba
2021-10-05T22:43:13.480	alert	172.16.1.102	53268	169.239.128.11	80	TCP	http	1	ET MALWARE MirrorBlast CnC Activity M3	Malware Command and
2021-10-05T22:43:13.480	alert	172.16.1.102	53268	169.239.128.11	80	TCP	http	2	ET USER_AGENTS Suspicious User-Agent (REBOL)	Potentially Ba
2021-10-05T22:43:12.252	alert	172.16.1.102	53267	169.239.128.11	80	TCP	http	1	ET MALWARE MirrorBlast CnC Activity M3	Malware Command and
2021-10-05T22:43:12.252	alert	172.16.1.102	53267	169.239.128.11	80	TCP	http	2	ET USER_AGENTS Suspicious User-Agent (REBOL)	Potentially Ba
2021-10-05T22:43:07.848	alert	172.16.1.102	53262	169.239.128.11	80	TCP	http	1	ET MALWARE MirrorBlast CnC Activity M3	Malware Command and
2021-10-05T22:43:07.848	alert	172.16.1.102	53262	169.239.128.11	80	TCP	http	2	ET USER_AGENTS Suspicious User-Agent (REBOL)	Potentially Ba
2021-10-05T22:43:06.619	alert	172.16.1.102	53261	169.239.128.11	80	TCP	http	1	ET MALWARE MirrorBlast CnC Activity M3	Malware Command and

support@zappiehost.com

Home New Zealand Servers South Africa Servers Chile Servers Other Billing Panel

Taking Hosting Seriously

Providing solid and high quality SSD servers
All at affordable prices

Get in Touch or See Pricing



Paypal
Accepting payments through paypal. A popular payment gateway



Bitcoin
Accepting payments through bitcoin. Where privacy matters



Instant setup
Your new vps will be provisioned automatically



Support
We strive to provide the best and quickest support

-INFORMATION I OBSERVED WHILE ON VIRUS TOTAL INDICATES THAT THE IP ADDRESS 169[.]239[.]128[.]11 IS CONNECTED TO THE THREAT GROUP 'TA505'. TA505 IS KNOWN FOR FREQUENTLY CHANGING MALWARE, DRIVING GLOBAL TRENDS IN CRIMINAL MALWARE DISTRIBUTION, AND RANSOMWARE CAMPAIGNS INVOLVING CLOPS. ASSOCIATED GROUPS: HIVE0065, SPANDEX TEMPEST, CHIMBORAZO.

TA505

TA505 is a cyber criminal group that has been active since at least 2014. TA505 is known for frequently changing malware, driving global trends in criminal malware distribution, and ransomware campaigns involving Clop.^{[1][2][3][4][5]}

ID: G0092

① Associated Groups: Hive0065, Spandex Tempest, CHIMBORAZO

Version: 3.0

Created: 28 May 2019

Last Modified: 10 April 2024

[Version Permalink](#)

Associated Group Descriptions

Name	Description
Hive0065	[6]
Spandex Tempest	[7]
CHIMBORAZO	[7]

169.239.128.11

Score

Sign inSign up

DETECTIONDETAILSRELATIONS

COMMUNITY20

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contained in Graphs (10)

cert_esec

mirrorblast

2021-10-18 10:32:11

GeeG_RS

Copy of MirrorBlast TA505

2021-10-13 18:43:43

xxavier

hunt graph 1

2021-10-07 14:52:23

BushidoToken

MirrorBlast TA505

2021-09-27 21:40:13

S_Mickael

currentOski

2020-03-24 14:07:05

lior_bp

Gracewire

2020-01-30 15:32:09

cdareg

Untitled Graph

2019-12-05 11:24:01

raeezabdulla

TA505 Campaign

2019-10-31 08:33:32

cdareg

Untitled Graph

2019-10-10 12:01:51

aadi369

Microsoft Themed TA505 malicious domains

2019-10-09 09:54:53

Voting details (10)

ovidluu999

1 month ago

-1

minion30

4 months ago

+1

ballisticbear


6 months ago

-1

-MALWARE FAMILY: MIRRORBLAST: METHOD: WEAPONIZED EXCEL DOCUMENTS. PAYLOAD: THE MALICIOUS EXCEL MACROS WOULD DOWNLOAD & EXECUTE OTHER MALICIOUS FILES INCLUDING THE MALWARE MIRRORBLAST.

 [Products](#) [Solutions](#) [Support and Services](#) [Company](#) [How To Buy](#)

[Support Portal](#) [English](#)

Search 

Support and Services / Symantec Security Center / Protection Bulletins / MirrorBlast uses phishing messages to target financial organizations

MirrorBlast uses phishing messages to target financial organizations

October 14, 2021 [Copy Link](#)

MirrorBlast is a new attack chain campaign targeting multiple financial service organizations in Canada, Europe, Hong Kong and the United States. The attackers utilize phishing emails with links to malicious Excel files. These files contain malicious macro code that executes the payload and evades detection while sending information to a command and control center server.

Symantec protects you from this threat, identified by the following:

Email-based

- Coverage is in place for Symantec's email security products






File-based

- Threat Artifact
- Trojan.Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malmsi
- Trojan.Mdropper
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

Web-based

- Observed domains are covered under security categories

-IN THE COMMUNICATING FILES SECTION IN VIRUS TOTAL I OBSERVED TWO FILES OF INTEREST: WIN32.EXE & WINDOWS INSTALLER.

 169.239.128.11     [Sign in](#) [Sign up](#)

Scanned	Detections	Type	Name
2022-11-20	0 / 94	VirusTotal	renauu.wiki
2022-04-07	8 / 94	VirusTotal	routinecmmrz.xyz
2022-04-07	0 / 94	VirusTotal	www.routinecmmrz.xyz
2022-04-03	0 / 94	VirusTotal	cmmrz-visit.xyz
2022-04-03	0 / 94	VirusTotal	www.cmmrz-visit.xyz

Communicating Files (188)

Scanned	Detections	Type	Name
2020-08-30	20 / 60	Office Open XML Spreadsheet	result.xlsx
2021-03-02	55 / 71	Win32 EXE	wotsuper3.exe
2020-08-07	43 / 73	Win32 EXE	wotsuper.exe
2020-08-28	53 / 68	Win32 EXE	bb62edbc434c9c35b8151035475f9a66.virus
2020-08-21	64 / 68	Win32 EXE	06c0c9101e4d3685a427.pe32
2021-04-12	53 / 70	Win32 EXE	tau111.exe
2020-02-27	33 / 72	Win32 EXE	Vidar.exe
2025-08-12	37 / 63	Windows Installer	10opd3r_load.msi
2025-03-24	62 / 73	Win32 EXE	FSTIME.EXE
2020-08-16	38 / 68	Win32 EXE	Vidar.exe

Files Referring (2)

Scanned	Detections	Type	Name
2022-05-16	0 / 57	Text	2021-10-05-MirrorBlast-IOCs.txt
2021-10-12	0 / 56	JavaScript	Case_Indicators_10.10.csv

Historical Whois Lookups (5)

Last Updated	Organization	Email
--------------	--------------	-------

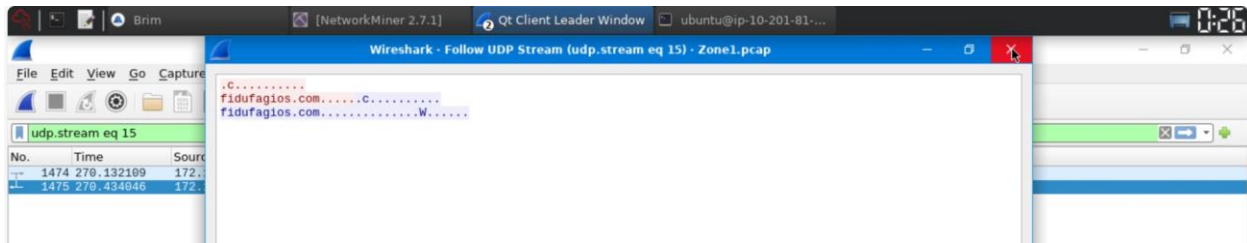
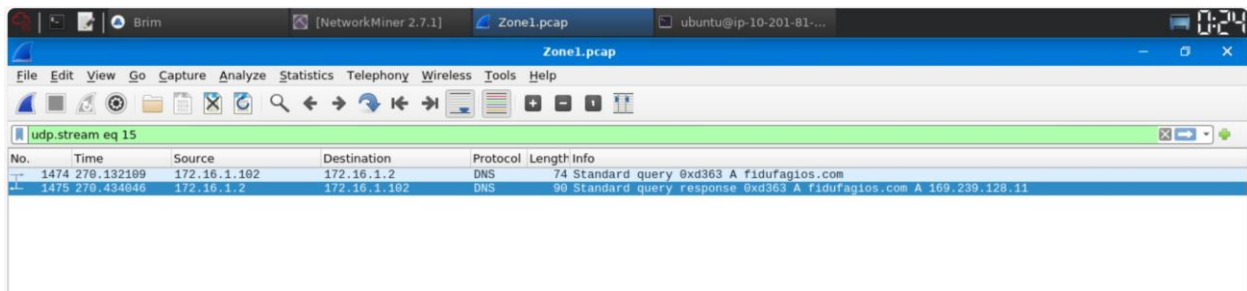
-I OBSERVED THAT THE ADVERSARY USED THE USER-AGENT 'REBOL VIEW 2.7.8.3.1'. A REPORT FROM 2021 ON REBOL EXPLOIT NOTED THE USER AGENT STRING 'REBOL VIEW 2.7.8.3.1' USED IN A MALICIOUS HTTP REQUEST.

```

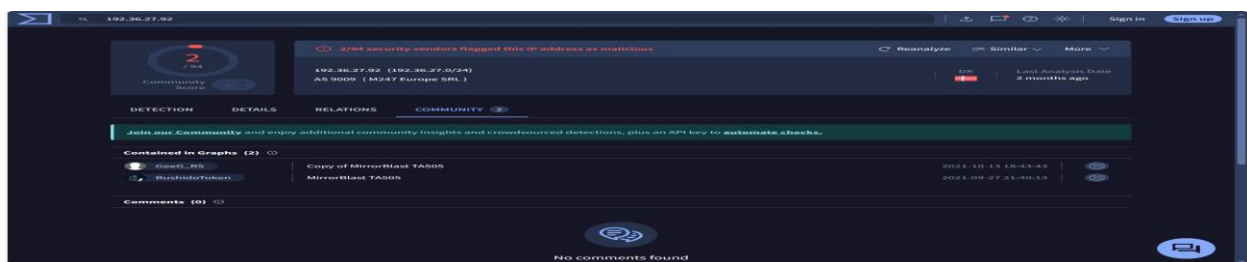
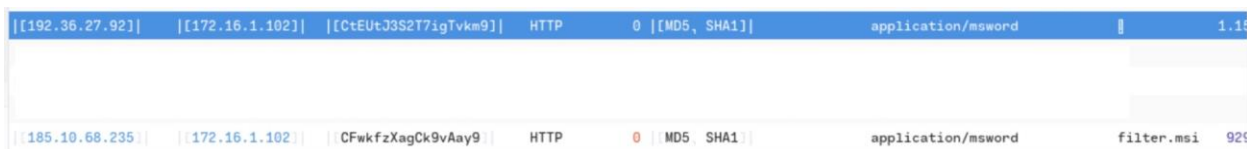
0 | TCP | http | 1 | ET MALWARE MirrorBlast CnC Activity M3 | Malware Command and Control Activity Detected | allowed | 2,034,023 | 1 | 2 | Major | MALWARE | C
0 | TCP | http | 2 | ET USER_AGENTS Suspicious User-Agent (REBOL) | Potentially Bad Traffic | allowed | 2,034,021 | 1 | 1 | Minor | USER_AGENTS | Client_Endpoi
0 | TCP | http | 1 | ET MALWARE MirrorBlast CnC Activity M3 | Malware Command and Control Activity Detected | allowed | 2,034,023 | 1 | 2 | Major | MALWARE | C
0 | TCP | http | 2 | ET USER_AGENTS Suspicious User-Agent (REBOL) | Potentially Bad Traffic | allowed | 2,034,021 | 1 | 1 | Minor | USER_AGENTS | Client_Endpoi
0 | TCP | http | 1 | ET MALWARE MirrorBlast CnC Activity M3 | Malware Command and Control Activity Detected | allowed | 2,034,023 | 1 | 2 | Major | MALWARE | C
0 | TCP | http | 2 | ET USER_AGENTS Suspicious User-Agent (REBOL) | Potentially Bad Traffic | allowed | 2,034,021 | 1 | 1 | Minor | USER_AGENTS | Client_Endpoi
0 | TCP | http | 1 | ET MALWARE MirrorBlast CnC Activity M3 | Malware Command and Control Activity Detected | allowed | 2,034,023 | 1 | 2 | Major | MALWARE | C

```

-THE IP ADDRESS: 169.239.128.11 CONNECTS TO FIDUFAGIOS[.]COM WHICH ACTS AS A C2 SERVER CONTROLLED BY THE ADVERSARY TA505.



-I OBSERVED THE ADVERSARY CONNECTED TO TWO OTHER IP ADDRESS: 192[.]36[.]27[.]92 & 185[.]10[.]68[.]235.



- THE ADVERSARIES MADE A CONNECTION TO 185[.]10[.]68[.]235 & DOWNLOADED 'FILTER.MSI' MIMICING A MICROSOFT WINDOWS INSTALLER TO DOWNLOAD & INSTALL TWO MORE FILES INTO THE SAME DIRECTORY C:\PROGRAMDATA\001\ARAB.BIN - C:\PROGRAMDATA\001\ARAB.EXE. THE ADVERSARIES ALSO CONNECTED TO 192[.]36[.]27[.]92 & DOWNLOADED 10OPD3R_LOAD.MSI AKA MIRRORBLAST A MALWARE LINKED TO PHISHING CAMPAIGN DATA EXFILTRATION. FURTHER FILES WERE DOWNLOADED: C:\PROGRADATA\LOCAL\GOOGLE\REBOL-VIEW-278-3-1.EXE - C:\PROGRAMDATA\LOCAL\GOOGLE\EXEMPLE.RB

oe6451e1f0eadb89390f4360e2a9a2fb66e92eb3ae75400095e75fd4dd6abb

37/63 security vendors flagged this file as malicious

Community Score: **37 / 63**

Size: **548.00 KB** | Last Analysis Date: **11 days ago** | MSI

File Name: **10opd3r_load.msi**

Tags: **msi malware checks-usb-bus direct-cpu-clock-access runtime-modules**

Tabs: DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY (17)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: **trojan.mirrorblast/ruby** | Threat categories: trojan, downloader | Family labels: mirrorblast, ruby, dwnld

Security vendors' analysis

Vendor	Detection	Category	Family Label
AhnLab-V3	Downloader/MSI.Generic	AliCloud	Trojan[downloader]/MSOffice/MirrorBlas...
ALYac	Trojan.Downloader.MSI.Agent	Antiy-AVL	Trojan[Downloader]/Ruby.TAS05
Arcabit	Trojan.Generic.D2CEF0D6	Avast	Other-Malware-gen [Trj]
AVG	Other.Malware-gen [Trj]	Avira (no cloud)	TR/Agent_ptw
BkDefender	Trojan.Generic.KD.47116445	CTX	Msi.trojan.mirrorblast
Cynet	Malicious (score: 99)	DrWeb	Ruby.Downloader.2

```

11mEnum_CostFinalizeFileCostCostFinalizeInstallValidateInstallInitializeInstallAdminPackageInstallFilesInsta
12Internet Protocol Version
13Transmission Control Prot
14
1511mEnum_CostFinalizeFileCostCostFinalizeInstallValidateInstallInitializeInstallAdminPackageInstallFilesInsta
1611FinalizeExecuteActionPublishFeaturesPublishProductComponent_CommonAppDataFolder(DEA88988-9EB8-4997-
17B469-148BA2A13D95)CommonAppDataFolderComponent.INSTALLDIR(DEA88988-9EB8-4997-B469-148B177F6F37)
18INSTALLDIRComponent.arab.bin(DEA88988-9EB8-4997-B469-148B85EDB3C2)
19arab.binComponent.arab.exe(DEA88988-9EB8-4997-B469-148B83B5B3B3)
20arab.exeTempFolder.EmptyDirectory(DEA88988-9EB8-4997-B469-148BA7A3C431)
21TempFolder.reg79EC0D928069C366464022E297B6TAGETDIR(DEA88988-9EB8-4997-B469-148B57246387)Action1_arab.exe3
22ProgramData9891arab.bin09613526CommonAppDataFolder19mu-pt
23TempFolderSourceDirWK1K32_WK1K32_660_01033ValidateProductIDProcessComponentsUnpublishFeaturesRemoveRegistryV
24aluesRemoveFilesRemoveFoldersCreateFoldersWriteRegistryValues(NOT
25Installed)_64545_.cabManufacturerProductCode(DEA88988-9EB8-4997-B469-148BF4540314)
26ProductLanguageProductName64545ProductVersion1_0_0UpgradeCode{6E17A28F-8D23-4F70-8404-1A5CA4EB63F7}
27Software\WishSharp\Usedup
28
290000 00 1f 3b 33 06 c0 20
300010 05 dc c2 1b 00 00 80
310020 01 66 00 50 cf ee af
320030 fa f9 59 22 00 00 2d
330040 2d 42 34 36 39 2d 31
340050 33 31 7d 54 65 6d 70
350060 35 37 39 45 43 38 44
360070 30 36 34 36 41 34 39
370080 54 41 52 47 45 54 30
38
39Packet 174, 1 client pkt(s), 139 server pkt(s), 1 turn(s). Click to select.

```

CONCLUSION:

THE INVESTIGATION INTO THE PCAP FILE 'ZONE1.PCAP' CONFIRMED SUSPICIOUS NETWORK ACTIVITY CONSISTENT WITH MALWARE COMMAND AND CONTROL (C2) TRAFFIC. THE ALERT "ET MALWARE MIRRORBLAST CNC ACTIVITY M3" WAS VALIDATED, LINKING THE INCIDENT TO THE THREAT GROUP TA505, A WELL-KNOWN THREAT ACTOR ASSOCIATED WITH GLOBAL MALWARE DISTRIBUTION AND RANSOMWARE CAMPAIGNS.

KEY FINDINGS INCLUDE THE USE OF THE IP ADDRESS 169[.]239[.]128[.]11, HOSTED BY ZAPPIE HOST LLC AND GEOLOCATED TO SOUTH AFRICA, WHICH WAS OBSERVED ACTING AS A C2 SERVER FOR THE ADVERSARY. THE USER-AGENT STRING "REBOL VIEW 2.7.8.3.1" WAS OBSERVED IN CONNECTIONS, MATCHING KNOWN MALICIOUS INDICATORS LINKED TO REBOL EXPLOITATION.

THE ADVERSARY ALSO UTILIZED SECONDARY INFRASTRUCTURE AT 185[.]10[.]68[.]235 AND 192[.]36[.]27[.]92 TO DELIVER ADDITIONAL MALICIOUS PAYLOADS, INCLUDING FILTER.MSI AND 10OPD3R_LOAD.MSI, WHICH FURTHER DROPPED EXECUTABLES AND BINARIES INTO SYSTEM DIRECTORIES. OBSERVED MALICIOUS FILES INCLUDE ARAB.BIN, ARAB.EXE, REBOL-VIEW-278-3-1.EXE, AND EXEMPLE.RB.

BASED ON THE TRAFFIC ANALYSIS, SIGNATURE ALERTS, AND FILE OBSERVATIONS, THIS INCIDENT IS CONFIRMED AS A COMPROMISE EVENT INVOLVING MIRRORBLAST MALWARE FAMILY.

THE PRIMARY INFECTION VECTOR APPEARS TO BE WEAPONIZED EXCEL DOCUMENTS LEADING TO PAYLOAD EXECUTION AND FOLLOW-UP C2 COMMUNICATIONS.

THE INCIDENT POSES A SIGNIFICANT RISK OF DATA EXFILTRATION, LATERAL MOVEMENT, AND FOLLOW-ON RANSOMWARE DEPLOYMENT, GIVEN TA505'S HISTORY WITH CLOP AND RELATED CAMPAIGNS. IMMEDIATE REMEDIATION, INCLUDING ISOLATION OF THE AFFECTED HOST (172[.]16[.]1[.]102), BLOCKING THE MALICIOUS IP ADDRESSES, AND SCANNING FOR INDICATORS OF COMPROMISE (IOCS), IS RECOMMENDED.