VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR

Crowdsourced YARA rules

⚠ Matches rule Base64_Encoded_URL from ruleset Base64_Encoded_URL by InQuest Labs

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

⚠ Matches rule Office Application Initiated Network Connection To Non-Local IP by Christopher Peacock '@securepeacock', SCYTHE '@scythe_io', Florian Roth (Nextron Systems), Tim Shelton, Nasreddine Bencherchali (Nextron Systems)

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected
AliCloud	✓ Undetected
ALYac	✓ Undetected
Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected
Avast	✓ Undetected
AVG	✓ Undetected
Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected
BitDefender	✓ Undetected
Bkav Pro	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
CrowdStrike Falcon	✓ Undetected
CTX	✓ Undetected
Cynet	✓ Undetected
DrWeb	✓ Undetected
Emsisoft	✓ Undetected
eScan	✓ Undetected
ESET-NOD32	✓ Undetected

Fortinet	✓ Undetected
GData	✓ Undetected
Google	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected
Huorong	✓ Undetected
Ikarus	✓ Undetected
Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected
K7GW	✓ Undetected
Kaspersky	✓ Undetected
Kingsoft	✓ Undetected
Lionic	✓ Undetected
Malwarebytes	✓ Undetected
MaxSecure	✓ Undetected
McAfee Scanner	✓ Undetected
Microsoft	✓ Undetected
NANO-Antivirus	✓ Undetected
Panda	✓ Undetected
QuickHeal	✓ Undetected
Rising	✓ Undetected
Sangfor Engine Zero	✓ Undetected
Skyhigh (SWG)	✓ Undetected
Sophos	✓ Undetected
SUPERAntiSpyware	✓ Undetected
Symantec	✓ Undetected
TACHYON	✓ Undetected
Tencent	✓ Undetected
Trellix ENS	✓ Undetected
TrendMicro	✓ Undetected
TrendMicro-HouseCall	✓ Undetected
Varist	✓ Undetected
VBA32	✓ Undetected
VIPRE	✓ Undetected
VirIT	✓ Undetected
ViRobot	✓ Undetected
WithSecure	✓ Undetected
Xcitium	✓ Undetected
Yandex	✓ Undetected
Zillya	✓ Undetected
ZoneAlarm by Check Point	✓ Undetected
Zoner	✓ Undetected

Alibaba	Unable to process file type
Arctic Wolf	Unable to process file type
Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type
DeepInstinct	Unable to process file type
Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type
Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Trustlook	Unable to process file type
Webroot	Unable to process file type