JOINT
CYBERSECURITY
ADVISORY

Coauthored by:

TLP:WHITE

Product ID: A22-216A

August 4, 2022

2021 Top Malware Strains

SUMMARY

This joint Cybersecurity Advisory (CSA) was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Australian Cyber Security Centre (ACSC). This advisory provides details on the top malware strains observed in 2021.

Malware, short for "malicious software," can compromise a system by performing an unauthorized function or process. Malicious cyber actors often use malware to covertly compromise and then gain access to a computer or mobile device. Some examples of malware include viruses, worms, Trojans, ransomware, spyware, and rootkits.[1]

Immediate Actions You Can Take Now to Protect Against Malware:

- Patch all systems and prioritize patching known exploited vulnerabilities.
- Enforce multifactor authentication (MFA).
- Secure Remote Desktop Protocol (RDP) and other risky services.
- Make offline backups of your data.
- Provide end-user awareness and training about social engineering and phishing.

In 2021, the top malware strains included remote access Trojans (RATs), banking Trojans, information stealers, and ransomware. Most of the top malware strains have been in use for more than five years with their respective code bases evolving into multiple variations. The most prolific malware users are cyber criminals, who use malware to deliver ransomware or facilitate theft of personal and financial information.

CISA and ACSC encourage organizations to apply the recommendations in the Mitigations sections of this joint CSA. These mitigations include applying timely patches to systems, implementing user training, securing Remote Desktop Protocol (RDP), patching all systems especially for known exploited vulnerabilities, making offline backups of data, and enforcing multifactor authentication (MFA).

U.S. organizations: *to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.* ***Australian organizations*** *should report incidents to the Australian Signals Directorate's (ASD's) ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1).*

TECHNICAL DETAILS

Key Findings

The top malware strains of 2021 are: Agent Tesla, AZORult, Formbook, Ursnif, LokiBot, MOUSEISLAND, NanoCore, Qakbot, Remcos, TrickBot and GootLoader.

- Malicious cyber actors have used Agent Tesla, AZORult, Formbook, LokiBot, NanoCore, Remcos, and TrickBot for at least five years.
- Malicious cyber actors have used Qakbot and Ursnif for more than a decade.

Updates made by malware developers, and reuse of code from these malware strains, contribute to the malware's longevity and evolution into multiple variations. Malicious actors' use of known malware strains offers organizations opportunities to better prepare, identify, and mitigate attacks from these known malware strains.

The most prolific malware users of the top malware strains are cyber criminals, who use malware to deliver ransomware or facilitate theft of personal and financial information.

- Qakbot and TrickBot are used to form botnets and are developed and operated by Eurasian cyber criminals known for using or brokering botnet-enabled access to facilitate highly lucrative ransomware attacks. Eurasian cyber criminals enjoy permissive operating environments in Russia and other former Soviet republics.
- According to U.S. government reporting, TrickBot malware often enables initial access for Conti ransomware, which was used in nearly 450 global ransomware attacks in the first half of 2021. As of 2020, malicious cyber actors have purchased access to systems compromised by TrickBot malware on multiple occasions to conduct cybercrime operations.
- In 2021, cyber criminals conducted mass phishing campaigns with Formbook, Agent Tesla, and Remcos malware that incorporated COVID-19 pandemic themes to steal personal data and credentials from businesses and individuals.

In the criminal malware industry, including malware as a service (MaaS), developers create malware that malware distributors often broker to malware end-users.[2] Developers of these top 2021 malware strains continue to support, improve, and distribute their malware over several years. Malware developers benefit from lucrative cyber operations with low risk of negative consequences. Many malware developers often operate from locations with few legal prohibitions against malware development and deployment. Some developers even market their malware products as legitimate cyber security tools. For example, the developers of Remcos and Agent Tesla have marketed the software as legitimate tools for remote management and penetration testing. Malicious cyber actors can purchase Remcos and Agent Tesla online for low cost and have been observed using both tools for malicious purposes.

Top Malware

Agent Tesla

- **Overview:** Agent Tesla is capable of stealing data from mail clients, web browsers, and File Transfer Protocol (FTP) servers. This malware can also capture screenshots, videos, and

Windows clipboard data. Agent Tesla is available online for purchase under the guise of being a legitimate tool for managing your personal computer. Its developers continue to add new functionality, including obfuscation capabilities and targeting additional applications for credential stealing.[3][4]

- **Active Since:** 2014
- **Malware Type:** RAT
- **Delivery Method:** Often delivered as a malicious attachment in phishing emails.
- **Resources:** See the MITRE ATT&CK page on Agent Tesla.

AZORult

- **Overview:** AZORult is used to steal information from compromised systems. It has been sold on underground hacker forums for stealing browser data, user credentials, and cryptocurrency information. AZORult's developers are constantly updating its capabilities.[5][6]
- **Active Since:** 2016
- **Malware Type:** Trojan
- **Delivery Method:** Phishing, infected websites, exploit kits (automated toolkits exploiting known software vulnerabilities), or via dropper malware that downloads and installs AZORult.
- **Resources:** See the MITRE ATT&CK page on AZORult and the Department of Health and Human Services (HHS)'s AZORult brief.

FormBook

- **Overview:** FormBook is an information stealer advertised in hacking forums. ForrmBook is capable of key logging and capturing browser or email client passwords, but its developers continue to update the malware to exploit the latest Common Vulnerabilities and Exposures (CVS)[7], such as CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability.[8][9]
- **Active Since:** At least 2016
- **Malware Type:** Trojan
- **Delivery Method:** Usually delivered as an attachment in phishing emails.
- **Resources:** See Department of Health and Human Services (HHS)'s Sector Note on Formbook Malware Phishing Campaigns.

Ursnif

- **Overview:** Ursnif is a banking Trojan that steals financial information. Also known as Gozi, Ursnif has evolved over the years to include a persistence mechanism, methods to avoid sandboxes and virtual machines, and search capability for disk encryption software to attempt key extraction for unencrypting files.[10][11][12] Based on information from trusted third parties, Ursnif infrastructure is still active as of July 2022.
- **Active Since:** 2007
- **Malware Type:** Trojan
- **Delivery Method:** Usually delivered as a malicious attachment to phishing emails.
- **Resources:** See the MITRE ATT&CK page on Ursnif.

LokiBot

- **Overview:** LokiBot is a Trojan malware for stealing sensitive information, including user credentials, cryptocurrency wallets, and other credentials. A 2020 LokiBot variant was disguised as a launcher for the Fortnite multiplayer video game.[13][14]
- **Active Since:** 2015
- **Malware Type:** Trojan
- **Delivery Method:** Usually delivered as a malicious email attachment.
- **Resources:** See CISA's LokiBot Malware alert and the MITRE ATT&CK page on LokiBot.

MOUSEISLAND

- **Overview:** MOUSEISLAND is usually found within the embedded macros of a Microsoft Word document and can download other payloads. MOUSEISLAND may be the initial phase of a ransomware attack.[15]
- **Active Since:** At least 2019
- **Malware Type:** Macro downloader
- **Delivery Method:** Usually distributed as an email attachment.
- **Resources:** See Mandiant's blog discussing MOUSEISLAND.

NanoCore

- **Overview:** NanoCore is used for stealing victims' information, including passwords and emails. NanoCore could also allow malicious users to activate computers' webcams to spy on victims. Malware developers continue to develop additional capabilities as plug-ins available for purchase or as a malware kit or shared amongst malicious cyber actors.[16][17][18]
- **Active Since:** 2013
- **Malware Type:** RAT
- **Delivery Method:** Has been delivered in an email as an ISO disk image within malicious ZIP files; also found in malicious PDF documents hosted on cloud storage services.
- **Resources:** See the MITRE ATT&CK page on NanoCore and the HHS Sector Note: Remote Access Trojan Nanocore Poses Risk to HPH Sector.

Qakbot

- **Overview:** originally observed as a banking Trojan, Qakbot has evolved in its capabilities to include performing reconnaissance, moving laterally, gathering and exfiltrating data, and delivering payloads. Also known as QBot or Pinksliplot, Qakbot is modular in nature enabling malicious cyber actors to configure it to their needs. Qakbot can also be used to form botnets.[19][20]
- **Active Since:** 2007
- **Malware Type:** Trojan
- **Delivery Method:** May be delivered via email as malicious attachments, hyperlinks, or embedded images.
- **Resources:** See the MITRE ATT&CK page on Qakbot and the Department of Health and Human Services (HHS) Qbot/Qakbot Malware brief.

Remcos

- **Overview:** Remcos is marketed as a legitimate software tool for remote management and penetration testing. Remcos, short for Remote Control and Surveillance, was leveraged by malicious cyber actors conducting mass phishing campaigns during the COVID-19 pandemic to steal personal data and credentials. Remcos installs a backdoor onto a target system. Malicious cyber actors then use the Remcos backdoor to issue commands and gain administrator privileges while bypassing antivirus products, maintaining persistence, and running as legitimate processes by injecting itself into Windows processes.[21][22]
- **Active Since:** 2016
- **Malware Type:** RAT
- **Delivery Method:** Usually delivered in phishing emails as a malicious attachment.
- **Resources:** See the MITRE ATT&CK page on Remcos.

TrickBot

- **Overview:** TrickBot malware is often used to form botnets or enabling initial access for the Conti ransomware or Ryuk banking trojan. TrickBot is developed and operated by a sophisticated group of malicious cyber actors and has evolved into a highly modular, multi-stage malware. In 2020, cyber criminals used TrickBot to target the Healthcare and Public Health (HPH) Sector and then launch ransomware attacks, exfiltrate data, or disrupt healthcare services. Based on information from trusted third parties, TrickBot's infrastructure is still active in July 2022.[23][24][25][26]
- **Active Since:** 2016
- **Malware Type:** Trojan
- **Delivery Method:** Usually delivered via email as a hyperlink.
- **Resources:** See the MITRE ATT&CK page on Trickbot and the Joint CSA on TrickBot Malware.

GootLoader

- **Overview:** GootLoader is a malware loader historically associated with the GootKit malware. As its developers updated its capabilities, GootLoader has evolved from a loader downloading a malicious payload into a multi-payload malware platform. As a loader malware, GootLoader is usually the first-stage of a system compromise. By leveraging search engine poisoning, GootLoader's developers may compromise or create websites that rank highly in search engine results, such as Google search results.[27]
- **Active Since:** At least 2020
- **Malware Type:** Loader
- **Delivery Method:** Malicious files available for download on compromised websites that rank high as search engine results
- **Resources:** See New Jersey's Cybersecurity & Communications Integration Cell (NJCCIC) page on GootLooader and BlackBerry's Blog on GootLoader.

MITIGATIONS

Below are the steps that CISA and ACSC recommend organizations take to improve their cybersecurity posture based on known adversary tactics, techniques, and procedures (TTPs). CISA

and ACSC urge critical infrastructure organizations to prepare for and mitigate potential cyber threats immediately by (1) updating software, (2) enforcing MFA, (3) securing and monitoring RDP and other potentially risky services, (4) making offline backups of your data, and (5) providing end-user awareness and training.

- **Update software, including operating systems, applications, and firmware, on IT network assets.** Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
    - Consider using a centralized patch management system.
    - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.
- **Enforce MFA** to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords. Do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. Additionally, ACSC has issued guidance on implementing multifactor authentication for hardening authentication systems.
- **If you use RDP and/or other potentially risky services, secure and monitor them closely.** RDP exploitation is one of the top initial infection vectors for ransomware, and risky services, including RDP, can allow unauthorized access to your session using an on-path attacker.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources, and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN) or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force attempts, log RDP login attempts, and disable unused remote access/RDP ports.
    - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- **Maintain offline (i.e., physically disconnected) backups of data**. Backup procedures should be conducted on a frequent, regular basis (at a minimum every 90 days). Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.
    - Ensure the backup keys are kept offline as well, to prevent them being encrypted in a ransomware incident.

  - Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure with a particular focus on key data assets.

- **Provide end-user awareness and training** to help prevent successful targeted social engineering and spearphishing campaigns. Phishing is one of the top infection vectors for ransomware.
  - Ensure that employees are aware of potential cyber threats and delivery methods.
  - Ensure that employees are aware of what to do and whom to contact when they receive a suspected phishing email or suspect a cyber incident.

As part of a longer-term effort, **implement network segmentation to separate network segments based on role and functionality**. Network segmentation can help prevent the spread of ransomware and threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks. The ACSC has observed ransomware and data theft incidents in which Australian divisions of multinational companies were impacted by ransomware incidents affecting assets maintained and hosted by offshore divisions outside their control.

RESOURCES

- For alerts on malicious and criminal cyber activity, see the FBI Internet Crime Complaint Center webpage.
- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. Government webpage providing ransomware resources and alerts.
- The ACSC recommends organizations implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a cybersecurity baseline. These strategies, known as the "Essential Eight," make it much harder for adversaries to compromise systems.
- Refer to the ACSC's practical guides on how to protect yourself against ransomware attacks and what to do if you are held at ransom at cyber.gov.au.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and ACSC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.

REFERENCES

[1] Malware Tip Card

[2] Malware Trends

[3] Agent Telsa

[4] Agent Tesla Trojan 'Kneecaps' Microsoft's Anti-Malware Interface

[5] AZORULT Malware Information

[6] HHS AZORult Malware

[7] Cybersecurity and Vulnerabilities and Exposures (CVE) list

[8] Significant FormBook Distribution Campaigns Impacting the U.S. and South Korea

[9] FormBook Adds Latest Office 365 0-Day Vulnerability (CVE-2021-40444) to Its Arsenal

[10] Ursnif Trojan has targeted over 100 Italian banks

[11] New Variant of Ursnif Continuously Targeting Italy

[12] URSNIF

[13] LokiBot trojan malware campaign comes disguised as a popular game launcher

[14] CISA and MS-ISAC LokiBot Malware

[15] So Unchill: Melting UNC2198 ICEDID to Ransomware Operations

[16] Nanocore, Netwire, and AsyncRAT spreading campaign uses public cloud infrastructure

[17] LokiBot & NanoCore being distributed via ISO disk image files

[18] U.S. Department of Justice: Arkansas Man Sentenced to Prison for Developing and Distributing Prolific Malware

[19] A closer look at Qakbot's latest building blocks (and how to knock them down)

[20] The rise of QakBot

[21] Remcos Malware Information

[22] The Latest Remcos RAT Driven By Phishing Campaign

[23] HHS The Evolution of Ryuk

[24] CISA Fact Sheet: TrickBot Malware

[25] Joint CSA Conti Ransomware

[26] Joint CSA Ransomware Activity Targeting the Healthcare and Public Health Sector

[27] New Jersey's Cybersecurity & Communications Integration Cell (NJCCIC) page on GootLooader

APPENDIX: SNORT SIGNATURES FOR THE TOP 2021 MALWARE

Malware	Snort Detection Signature
Agent Tesla	alert any any -> any any (msg:"HTTP GET request /aw/aw.exe"; flow:established,to_server; sid:1; rev:1; content:"GET"; http_method;

Malware	Snort Detection Signature
	content:"/aw/aw.exe"; http_uri; reference:url, https://www.datto.com/blog/what-is-agent-tesla-spyware-and-how-does-it-work; metadata:service http;)
AZORult	alert tcp any any -> any any (msg:"HTTP Server Content Data contains 'llehS|2e|tpircSW'"; sid:1; rev:1; flow:established,from_server; file_data; content:"llehS|2e|tpircSW"; nocase; fast_pattern:only; pcre:"/GCM(?:\x20|%20)*W-O*/i"; reference:url,maxkersten.nl/binary-analysis-course/malware-analysis/azorult-loader-stages/; metadata:service http;)
AZORult	alert tcp any any -> any any (msg:"HTTP POST Client Body contains 'J/|fb|' and '/|fb|'"; sid:1; rev:1; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"J/|fb|"; http_client_body; fast_pattern; content:"/|fb|"; http_client_body; depth:11; content:!"Referer|3a 20|"; http_header; metadata:service http;)
FormBook	alert tcp any any -> any any (msg:"HTTP URI POST contains '&sql=1' at the end"; sid:1; rev:1; flow:established,to_server; content:"&sql=1"; http_uri; fast_pattern:only; content:"POST"; http_method; pcre:"/(?(DEFINE)(?'b64std'[a-zA-Z0-9+\/=]+?))(?(DEFINE)(?'b64url'[a-zA-Z0-9_-]+?))^\/[a-z0-9]{3,4}\/\?(?P>b64url){3,8}=(?P>b64std){40,90}&(?P>b64url){2,6}=(?P>b64url){4,11}&sql=1$/iU"; reference:url,www.malware-traffic-analysis.net/2018/02/16/index.html; metadata:service http;)
	alert tcp any any -> any any (msg:"HTTP URI GET/POST contains '/list/hx28/config.php?id='"; sid:1; rev:1; flow:established,to_server; content:"/list/hx28/config.php?id="; http_uri; fast_pattern:only; content:"Connection|3a 20|close|0d 0a|"; http_header; reference:url,www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html; metadata:service http;)
Ursnif	alert tcp any any -> any any (msg:"HTTP POST Data contains .bin filename, long URI contains '/images/'"; sid:1; rev:1; flow:established,to_server; urilen:>60,norm; content:"/images/"; http_uri; depth:8; content:"POST"; nocase; http_method; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|upload_file|22 3b 20|filename=|22|"; http_client_body; content:"|2e|bin|22 0d 0a|"; http_client_body; distance:1; within:32; fast_pattern; reference:url,www.broadanalysis.com/2016/03/23/angler-ek-sends-data-stealing-payload/; metadata:service http;)
	alert tcp any any -> any any (msg:"HTTP URI GET/POST contains '/images/' plus random sub directories and an Image File (Ursnif)"; sid:1; rev:1; flow:established,to_server; content:"/images/"; http_uri; fast_pattern:only; content:!"Host: www.urlquery.net"; http_header; pcre:"/\/images(\/(?=[a-z0-9_]{0,22}[A-Z][a-z0-9_]{0,22}[A-Z])(?=[A-Z0-9_]{0,22}[a-z])[A-Za-z0-

Malware	Snort Detection Signature
	9_]{1,24}){5,20}\/[a-zA-Z0-9_]+\.(?:gif|jpeg|jpg|bmp)$/U"; metadata:service http)
LokiBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'User-Agent|3a 20|Mozilla/4.08 (Charon|3b| Inferno)'"; sid:1; rev:1; flow:established,to_server; content:"User-Agent|3a 20|Mozilla/4.08 (Charon|3b| Inferno)|0d 0a|"; http_header; fast_pattern:only; metadata:service http;)
LokiBot	alert tcp any any -> any any (msg:"HTTP URI POST contains '/*/fre.php' post-infection"; sid:1; rev:1; flow:established,to_server; content:"/fre.php"; http_uri; fast_pattern:only; urilen:<50,norm; content:"POST"; nocase; http_method; pcre:"/\/(?:alien|loky\d|donep|jemp|lokey|new2|loki|Charles|sev7n|dbwork|scroll\/NW|wrk|job|five\d?|donemy|animation\dkc|love|Masky|v\d|lifetn|Ben)\/fre\.php$/iU"; metadata:service http;)
LokiBot	alert tcp any any -> any any (msg:"HTTP URI POST contains '/w.php/'"; sid:1; rev:1; flow:established,to_server; content:"/w.php/"; http_uri; fast_pattern:only; content:"POST"; nocase; http_method; pcre:"/\/\w+\/w\.php\/[a-z]{13}$/iU"; metadata:service http;)
MOUSEISLAND	alert tcp any any -> any any (msg:"HTTP URI GET contains '/assets/<8-80 hex>/<4-16 alnum>?<3-6 alnum>='"; sid:9206287; rev:1; flow:established,to_server; content:"/assets/"; http_uri; fast_pattern:only; content:"HTTP/1.1|0d 0a|"; depth:256; content:!"|0d 0a|Cookie:"; content:!"|0d 0a|Referer:"; pcre:"/\/assets\/[a-fA-F0-9/]{8,80}\/[a-zA-Z0-9]{4,16}\?[a-z0-9]{3,6}=/U"; metadata:service http;)
NanoCore	alert tcp any any -> any 25 (msg:"SMTP Attachment Filename 'Packinglist-Invoice101.pps'"; sid:1; rev:1; flow:established,to_server,only_stream; content:"Content-Disposition|3a 20|attachment|3b|"; content:"Packinglist-Invoice101.pps"; nocase; distance:0; fast_pattern; pcre:"/Content-Disposition\x3a\x20attachment\x3b[\x20\t\r\n]+?(?:file)*?name=\x22*?Packinglist-Invoice101\.pps\x22*?/im"; reference:cve,2014-4114; reference:msb,MS14-060; reference:url,researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/; reference:url,www.fidelissecurity.com/sites/default/files/FTA_1017_Phishing_in_Plain_Sight-Body-FINAL.pdf; reference:url,www.fidelissecurity.com/sites/default/files/FTA_1017_Phishing_in_Plain_Sight-Appendix-FINAL.pdf;)
NanoCore	alert tcp any any -> any any (msg:"HTTP Client Header contains 'Host|3a 20|frankief hopto me' (GenericKD/Kazy/NanoCore/Recam)"; sid:1; rev:1; flow:established,to_server; content:"Host|3a 20|frankief|2e|hopto|2e|me|0d 0a|"; http_header; fast_pattern:only; metadata:service http;)

Malware	Snort Detection Signature
NanoCore	alert tcp any any -> any any (msg:"HTTP GET URI contains 'FAD00979338'"; sid:1; rev:1; flow:established,to_server; content:"GET"; http_method; content:"getPluginName.php?PluginID=FAD00979338"; fast_pattern; http_uri; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI GET /t?v=2&c= (Qakbot)"; sid:1; rev:1; flow:established,to_server; content:"/t?v=2&c="; http_uri; depth:9; fast_pattern; reference:url,www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf;)
Qakbot	alert tcp any any -> any 21 (msg:"Possible FTP data exfiltration"; sid:1; rev:1; flow:to_server,established; content:"STOR si_"; content:".cb"; within:50; reference:url,attack.mitre.org/techniques/T1020; reference:url,www.virustotal.com/en/file/3104ff71bf880bc40d096eca7d1ccc3f762ea6cc89743c6fef744fd76d441d1b/analysis/; metadata:service ftp-ctrlchan;)
Qakbot	alert tcp any any -> any any (msg:"Malicious executable download attempt"; sid:1; rev:1; flow:to_client,established; file_type:MSEXE; file_data; content:"|52 DB 91 CB FE 67 30 9A 8E 72 28 4F 1C A9 81 A1 AA BE AC 8D D9 AB E4 15 EF EA C6 73 89 9F CF 2E|"; fast_pattern:only; reference:url,virustotal.com/#/file/ad815edc045c779628db3a3397c559ca08f012216dfac4873f11044b2aa1537b/detection; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP POST URI contains 'odin/si.php?get&'"; sid:1; rev:1; flow:to_server,established; content:"/odin/si.php?get&"; fast_pattern:only; http_uri; content:"news_slist"; http_uri; content:"comp="; http_uri; reference:url,www.virustotal.com/en/file/478132b5c80bd41b8c11e5ed591fdf05d52e316d40f7c4abf4bfd25db2463dff/analysis/1464186685/; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI contains '/random750x750.jpg?x='"; sid:1; rev:1; flow:to_server,established; content:"/random750x750.jpg?x="; fast_pattern:only; http_uri; content:"&y="; http_uri; content:"Accept|3a 20|application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*|0d 0a|"; http_header; content:"Cache-Control|3a 20|no-cache|0d 0a|"; http_header; content:!"Accept-"; http_header; content:!"Referer"; http_header; reference:url,www.virustotal.com/en/file/1826dba769dad9898acd95d6bd026a0b55d0a093a267b481695494f3ab547088/analysis/1461598351/; metadata:service http;)

Malware	Snort Detection Signature
Qakbot	alert tcp any any -> any any (msg:"HTTP URI contains '/datacollectionservice.php3'"; sid:1; rev:1; flow:to_server,established; content:"/datacollectionservice.php3"; fast_pattern:only; http_uri; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP header contains 'Accept|3a 20|application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*|0d 0a|'"; sid:1; rev:1; flow:to_server,established; urilen:30<>35,norm; content:"btst="; http_header; content:"snkz="; http_header; content:"Accept|3a 20|application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*|0d 0a|"; fast_pattern:only; http_header; content:"Cache-Control|3a 20|no-cache|0d 0a|"; http_header; content:!"Connection"; http_header; content:!"Referer"; http_header; reference:url,www.virustotal.com/en/file/1826dba769dad9898acd95d6bd026a0b55d0a093a267b481695494f3ab547088/analysis/1461598351/; metadata:service http;)
Qakbot	alert tcp any any -> any 21 (msg:"Possible ps_dump FTP exfil"; sid:1; rev:1; flow:to_server,established; content:"ps_dump"; fast_pattern:only; pcre:"/ps_dump_[^_]+_[a-z]{5}\d{4}\x2Ekcb/smi"; reference:url,www.threatexpert.com/report.aspx?md5=8171d3223f89a495f98c4e3a65537b8f; metadata:service ftp;)
Qakbot	alert tcp any any -> any 21 (msg:"Possible seclog FTP exfil"; sid:1; rev:1; flow:to_server,established; content:"seclog"; fast_pattern:only; pcre:"/seclog_[a-z]{5}\d{4}_\d{10}\x2Ekcb/smi"; reference:url,www.threatexpert.com/report.aspx?md5=8171d3223f89a495f98c4e3a65537b8f; metadata:service ftp;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI contains '/cgi-bin/jl/jloader.pl'"; sid:1; rev:1; flow:to_server,established; content:"/cgi-bin/jl/jloader.pl"; fast_pattern:only; http_uri; reference:url,www.threatexpert.com/report.aspx?md5=8171d3223f89a495f98c4e3a65537b8f; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI contains '/cgi-bin/clientinfo3.pl'"; sid:1; rev:1; flow:to_server,established; content:"/cgi-bin/clientinfo3.pl"; fast_pattern:only; http_uri; reference:url,www.threatexpert.com/report.aspx?md5=8171d3223f89a495f98c4e3a65537b8f; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI contains '/u/updates.cb'"; sid:1; rev:1; flow:to_server,established; content:"/u/updates.cb"; fast_pattern:only; http_uri; pcre:"/^Host\x3A[^\r\n]+((up\d+)|(adserv))/Hmi";

Malware	Snort Detection Signature
	reference:url,www.threatexpert.com/report.aspx?md5=8171d3223f89a495f98c4e3a65537b8f; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP response content contains '|47 65 74 46 69 6C 65 46 72 6F 6D 52 65 73 6F 75 72 63 65 73 28 29 3A 20 4C 6F 61 64 52 65 73 6F 75 72 63 65 28 29 20 66 61 69 6C 65 64|'"; sid:1; rev:1; flow:to_client,established; file_data; content:"|47 65 74 46 69 6C 65 46 72 6F 6D 52 65 73 6F 75 72 63 65 73 28 29 3A 20 4C 6F 61 64 52 65 73 6F 75 72 63 65 28 29 20 66 61 69 6C 65 64|"; fast_pattern:only; content:"|47 65 74 46 69 6C 65 46 72 6F 6D 52 65 73 6F 75 72 63 65 73 28 29 3A 20 43 72 65 61 74 65 46 69 6C 65 28 29 20 66 61 69 6C 65 64|"; content:"|52 75 6E 45 78 65 46 72 6F 6D 52 65 73 28 29 20 73 74 61 72 74 65 64|"; content:"|73 7A 46 69 6C 65 50 61 74 68 3D|"; content:"|5C 25 75 2E 65 78 65|"; reference:url,www.virustotal.com/en/file/23e72e8b5e7856e811a326d1841bd2ac27ac02fa909d0a951b0b8c9d1d6aa61c/analysis; metadata:service ftp-data,service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP POST URI contains 'v=3&c='"; sid:1; rev:1; flow:to_server,established; content:"/t"; http_uri; content:"POST"; http_method; content:"v=3&c="; depth:6; http_client_body; content:"=="; within:2; distance:66; http_client_body; reference:url,www.virustotal.com/en/file/3104ff71bf880bc40d096eca7d1ccc3f762ea6cc89743c6fef744fd76d441d1b/analysis/; metadata:service http;)
Qakbot	alert tcp any any -> any any (msg:"HTTP URI GET contains '/<alpha>/595265.jpg'"; sid:1; rev:1; flow:established,to_server; content:"/595265.jpg"; http_uri; fast_pattern:only; content:"GET"; nocase; http_method; pcre:"/^\/[a-z]{5,15}\/595265\.jpg$/U"; reference:url,www.virustotal.com/gui/file/3104ff71bf880bc40d096eca7d1ccc3f762ea6cc89743c6fef744fd76d441d1b/detection; metadata:service http;)
Remcos	alert tcp any any -> any any (msg:"Non-Std TCP Client Traffic contains '|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|' (Checkin #23)"; sid:1; rev:1; flow:established,to_server; dsize:<700; content:"|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|"; depth:11; fast_pattern; content:"|da b1|"; distance:2; within:2; reference:url,blog.trendmicro.com/trendlabs-security-intelligence/analysis-new-remcos-rat-arrives-via-phishing-email/; reference:url,isc.sans.edu/forums/diary/Malspam+using+passwordprotected+Word+docs+to+push+Remcos+RAT/25292/; reference:url,www.malware-traffic-analysis.net/2019/09/03/index.html; reference:url,www.malware-traffic-analysis.net/2017/10/27/index.html;)

Malware	Snort Detection Signature
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'host|3a 20|tpsci.com'"; sid:1; rev:1; flow:established,to_server; content:"host|3a 20|tpsci.com"; http_header; fast_pattern:only; metadata:service http;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'User-Agent|3a 20|*Loader'"; sid:1; rev:1; flow:established,to_server; content:"User-Agent|3a 20|"; http_header; content:"Loader|0d 0a|"; nocase; http_header; distance:0; within:24; fast_pattern; metadata:service http;)
TrickBot	alert udp any any <> any 53 (msg:"DNS Query/Response onixcellent com (UDP)"; sid:1; rev:1; content:"|0B|onixcellent|03|com|00|"; fast_pattern:only; reference:url,medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30; priority:1; metadata:service dns;)
TrickBot	alert tcp any any -> any any (msg:"SSL/TLS Server X.509 Cert Field contains 'C=XX, L=Default City, O=Default Company Ltd'"; sid:1; rev:2; flow:established,from_server; ssl_state:server_hello; content:"|31 0b 30 09 06 03 55 04 06 13 02|XX"; nocase; content:"|31 15 30 13 06 03 55 04 07 13 0c|Default City"; nocase; content:"|31 1c 30 1a 06 03 55 04 0a 13 13|Default Company Ltd"; nocase; content:!"|31 0c 30 0a 06 03 55 04 03|"; reference:url,www.virustotal.com/gui/file/e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
TrickBot	alert tcp any any -> any any (msg:"SSL/TLS Server X.509 Cert Field contains 'C=AU, ST=Some-State, O=Internet Widgits Pty Ltd'"; sid:1; rev:1; flow:established,from_server; ssl_state:server_hello; content:"|31 0b 30 09 06 03 55 04 06 13 02|AU"; content:"|31 13 30 11 06 03 55 04 08 13 0a|Some-State"; distance:0; content:"|31 21 30 1f 06 03 55 04 0a 13 18|Internet Widgits Pty Ltd"; distance:0; fast_pattern; content:"|06 03 55 1d 13 01 01 ff 04 05 30 03 01 01 ff|"; reference:url,www.virustotal.com/gui/file/e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'boundary=Arasfjasu7'"; sid:1; rev:1; flow:established,to_server; content:"boundary=Arasfjasu7|0d 0a|"; http_header; content:"name=|22|proclist|22|"; http_header; content:!"Referer"; content:!"Accept"; content:"POST"; http_method; metadata:service http;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'User-Agent|3a 20|WinHTTP loader/1.'"; sid:1; rev:1; flow:established,to_server; content:"User-Agent|3a 20|WinHTTP loader/1."; http_header; fast_pattern:only; content:".png|20|HTTP/1."; pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}(?:\x3a\d{2,5})?$/mH";

Malware	Snort Detection Signature
	content:!"Accept"; http_header; content:!"Referer|3a 20|"; http_header; metadata:service http;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Server Header contains 'Server|3a 20|Cowboy'"; sid:1; rev:1; flow:established,from_server; content:"200"; http_stat_code; content:"Server|3a 20|Cowboy|0d 0a|"; http_header; fast_pattern; content:"content-length|3a 20|3|0d 0a|"; http_header; file_data; content:"/1/"; depth:3; isdataat:!1,relative; metadata:service http;)
TrickBot	alert tcp any any -> any any (msg:"HTTP URI POST contains C2 Exfil"; sid:1; rev:1; flow:established,to_server; content:"Content-Type|3a 20|multipart/form-data|3b 20|boundary=------Boundary"; http_header; fast_pattern; content:"User-Agent|3a 20|"; http_header; distance:0; content:"Content-Length|3a 20|"; http_header; distance:0; content:"POST"; http_method; pcre:"/^\/[a-z]{3}\d{3}\/.+?\.[A-F0-9]{32}\/\d{1,3}\//U"; pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}$/mH"; content:!"Referer|3a|"; http_header; metadata:service http;)
TrickBot	alert tcp any any -> any any (msg:"HTTP URI GET/POST contains '/56evcxv'"; sid:1; rev:1; flow:established,to_server; content:"/56evcxv"; http_uri; fast_pattern:only; metadata:service http;)
TrickBot	alert icmp any any -> any any (msg:"ICMP traffic conatins 'hanc'"; sid:1; rev:1; itype:8; icode:0; dsize:22; content:"hanc"; depth:4; fast_pattern; pcre:"/hanc[0-9a-f]{16}../i"; reference:url,labs.sentinelone.com/anchor-project-for-trickbot-adds-icmp/;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains POST with 'host|3a 20|*.onion.link' and 'data='"; sid:1; rev:1; flow:established,to_server; content:"POST"; nocase; http_method; content:"host|3a 20|"; http_header; content:".onion.link"; nocase; http_header; distance:0; within:47; fast_pattern; file_data; content:"data="; distance:0; within:5; metadata:service http;)
TrickBot	alert tcp any 80 -> any any (msg:"Non-Std TCP Client Traffic contains PowerView Script Download String"; sid:1; rev:1; flow:established,from_server; content:"PowerView.ps1"; content:"PSReflect/master/PSReflect.psm1"; fast_pattern:only; content:"function New-InMemoryModule"; metadata:service else-ports;)
TrickBot	alert tcp any any -> any 445 (msg:"Non-Std TCP Client SMB Traffic contains '44783m8uh77g818_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl'"; sid:1; rev:1; flow:established,to_server; content:"44783m8uh77g818_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl"; fast_pattern:only; metadata:service netbios-ssn,service and-ports;)

Malware	Snort Detection Signature
TrickBot	alert tcp any any -> any [80,443,8082] (msg:"Non-Std TCP Client Traffic contains '--aksgja8s8d8a8s97'"; sid:1; rev:1; flow:established,to_server; content:"--aksgja8s8d8a8s97"; fast_pattern:only; content:"name=|22|proclist|22|"; metadata:service else-ports;)
TrickBot	alert tcp any any -> any any (msg:"HTTP Client Header contains 'User-Agent|3a 20|WinHTTP loader/1.0'"; sid:1; rev:1; flow:established,to_server; content:"User-Agent|3a 20|WinHTTP loader/1.0|0d 0a|"; http_header; fast_pattern:only; pcre:"/\/t(?:oler|able)\.png/U"; metadata:service http;)
TrickBot	alert tcp any any -> any [443,8082] (msg:"Non-Std TCP Client Traffic contains '_W<digits>.'"; sid:1; rev:1; flow:established,to_server; content:"_W"; fast_pattern:only; pcre:"/_W\d{6,8}\./"; metadata:service else-ports;)
TrickBot	alert tcp any [443,447] -> any any (msg:"SSL/TLS Server X.509 Cert Field contains 'example.com' (Hex)"; sid:1; rev:1; flow:established,from_server; ssl_state:server_hello; content:"|0b|example.com"; fast_pattern:only; content:"Global Security"; content:"IT Department"; pcre:"/(?:\x09\x00\xc0\xb9\x3b\x93\x72\xa3\xf6\xd2|\x00\xe2\x08\xff\xfb\x7b\x53\x76\x3d)/"; metadata:service ssl,service and-ports;)
TrickBot	alert tcp any any -> any any+F57 (msg:"HTTP URI GET contains '/anchor'"; sid:1; rev:1; flow:established,to_server; content:"/anchor"; http_uri; fast_pattern:only; content:"GET"; nocase; http_method; pcre:"/^\/anchor_?.{3}\/[\w_-]+\.[A-F0-9]+\/?$/U"; metadata:service http;)
TrickBot	alert udp any any <> any 53 (msg:"DNS Query/Response kostunivo com (UDP)"; sid:1; rev:1; content:"|09|kostunivo|03|com|00|"; fast_pattern:only; reference:url,medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30; metadata:service dns;)
TrickBot	alert udp any any <> any 53 (msg:"DNS Query/Response chishir com (UDP)"; sid:1; rev:1; content:"|07|chishir|03|com|00|"; fast_pattern:only; reference:url,medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30; metadata:service dns;)
TrickBot	alert udp any any <> any 53 (msg:"DNS Query/Response mangoclone com (UDP)"; sid:1; rev:1; content:"|0A|mangoclone|03|com|00|"; fast_pattern:only; reference:url,medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30; metadata:service dns;)
GootLoader	No signature available.