THREAT BULLETIN

Anomali Cyber Watch: 2022-03-21

TLP
N/A

PUBLICATION STATUS
Published

PUBLISHED DATE
21 Mar 2022 20:49:47

VISIBILITY
Anomali Community

TAGS
magazine palo

DESCRIPTION

Anomali Cyber Watch: Russia Targets Ukraine with New Malware, Targeted Phishing Campaigns Give Way to Wizard Spider, Certificates Stolen by Lapsus$ Are Being Abused, and More.

The various threat intelligence stories in this iteration of the Anomali Cyber Watch discuss the following topics: **APT, Code signing, Naver, Phishing, Russia, Ukraine,** and **Vulnerabilities**. The IOCs related to these stories are attached to Anomali Cyber Watch and can be used to check your logs for potential malicious activity.

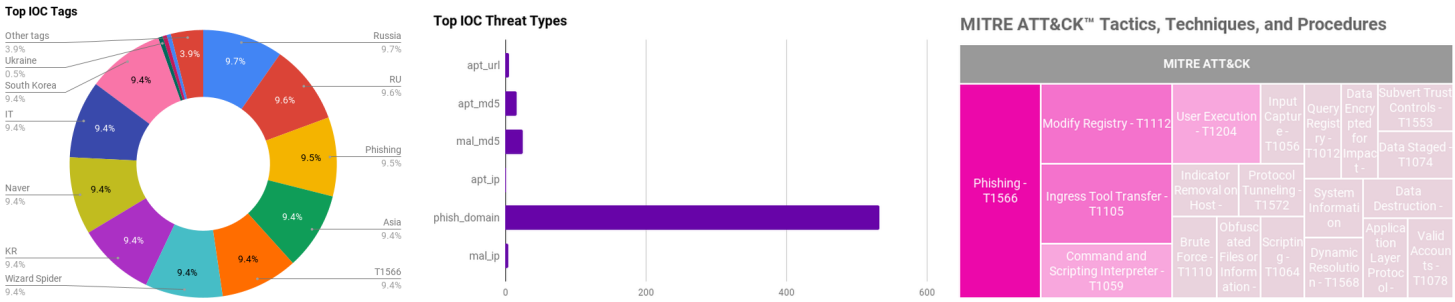

Figure 1 - IOC Summary Charts. These charts summarize the IOCs attached to this magazine and provide a glimpse of the threats discussed.

Trending Cyber News and Threat Intelligence

Double Header: IsaacWiper and CaddyWiper

(published: March 18, 2022)

Data destruction is one of the common objectives for Russia in its ongoing cyberwar with Ukraine. During the February-March 2022 military escalation, three new wipers were discovered. On February 23, 2022, HermeticWiper, on February 24, 2022, IsaacWiper, and, later in March 2022, CaddyWiper. Malwarebytes researchers assess that all three wipers have been written by different authors and have no code overlap. IsaacWiper and CaddyWiper are light in comparison to the more complex HermeticWiper. CaddyWiper has an additional check to exclude wiping Domain Controllers probably to leave an opportunity for malware propagation.
Analyst Comment: Focus on intrusion prevention and having a proper disaster recovery plan in place: have anti-phishing training, keep your systems updated, regularly backup your data to an offline storage.
MITRE ATT&CK: [MITRE ATT&CK] Data Destruction - T1485
Tags: CaddyWiper, IsaacWiper, HermeticWiper, Wiper, Data destruction, Russia, Ukraine, Ukraine-Russia Conflict 2022, Operation Bleeding Bear

UAC-0035 (InvisiMole) Attacks Ukrainian Government Organizations

(published: March 18, 2022)

The Computer Emergency Response Team for Ukraine (CERT-UA) detected a new UAC-0035 (InvisiMole) phishing campaign targeting Ukrainian government organizations. InvisiMole is likely a subgroup connected to the Russia-sponsored Gamaredon (Primitive Bear) group. The new campaign features an attached archive, together with a shortcut (LNK) file. If the LNK file is opened, an HTML Application file (HTA) downloads and executes VBScript designed to deploy the LoadEdge backdoor. LoadEdge deploys additional malware and modules including TunnelMole, malware that abuses the DNS protocol to form a tunnel for malicious software distribution, and RC2CL backdoor module.
Analyst Comment: Users should be trained to recognize spearphishing attempts. Attachments with rare attachment extensions (LNK, ISO, BAT to name a few) should be reported.

MITRE ATT&CK: [MITRE ATT&CK] Phishing - T1566 | [MITRE ATT&CK] Ingress Tool Transfer - T1105 | [MITRE ATT&CK] Protocol Tunneling - T1572 | [MITRE ATT&CK] Modify Registry - T1112 | [MITRE ATT&CK] User Execution - T1204
Tags: InvisiMole, UAC-0035, TunnelMole, Gamaredon, Primitive Bear, Russia, Ukraine, LNK, HTA, DNS, Ukraine-Russia Conflict 2022, Operation Bleeding Bear

Exposing Initial Access Broker with Ties to Conti

(published: March 17, 2022)

Exotic Lily (DEV-0413) is an initial access broker group detected by the Google Threat Analysis Group. Exotic Lily is capable of sending 5,000 emails a day, and has been observed targeting 650 organizations globally. The threat group relies heavily on human operations with manually spoofing organizations, creating fake employee profiles and personal websites. Exotic Lily tries to avoid detection by uploading their malicious payload to public file-sharing services such as OneDrive, TransferNow, TransferXL, or WeTransfer. In September 2021, Exotic Lily was sending an exploit for CVE-2021-40444. In or around November 2021, they switched to delivering ISO files with hidden BazarLoader DLLs and LNK shortcuts. Next infection stages include Cobalt Strike and deployment of Conti and Diavol ransomware. Exotic Lily has close relationships with Wizard Spider (FIN12) but seems to operate as a separate entity.
Analyst Comment: Users should be made aware that a malicious link can come even from somebody that they had an established communication with. Financially-motivated groups like Exotic Lily show a high level of persistence and resourcefulness and a defense-in-depth approach is needed on defenders' side.
MITRE ATT&CK: [MITRE ATT&CK] Phishing - T1566 | [MITRE ATT&CK] Data Encrypted for Impact - T1486 | [MITRE ATT&CK] Ingress Tool Transfer - T1105 | [MITRE ATT&CK] System Information Discovery - T1082
Tags: Exotic Lily, DEV-0413, TransferNow, TransferXL, WeTransfer, OneDrive, CVE-2021-40444, Bumblebee loader, BazarLoader, Bazar, ISO, DLL, LNK, Cobalt Strike, Conti, Diavol, Ransomware, Wizard Spider, FIN12

Suspected DarkHotel APT Activity Update

(published: March 17, 2022)

An IP address reported in December 2021 as a part of the South Korean threat actor DarkHotel, remained active as part of spearphishing campaign targeting luxury hotels in Macao, China. This campaign started in November 2021 and lasted through January 18, 2022, possibly stopping as the planned conferences in the targeted area were canceled due to COVID-19-related measures. The campaign featured attached Excel documents with malicious, obfuscated macroses containing multiple loops to make the analysis more complex. When executed by the user the macros creates a scheduled task to collect and exfiltrate data. Additionally, the macros utilizes a known LOLBAS (living off the land binaries and scripts) technique to perform PowerShell command lines as trusted scripts.
Analyst Comment: Hotel guests using hotel WiFi should use a VPN to keep their network traffic encrypted. Hotel administrators should be trained to recognize spearphishing attempts and avoid enabling macroses in the non-warranted attachments.
MITRE ATT&CK: [MITRE ATT&CK] Phishing - T1566 | [MITRE ATT&CK] User Execution - T1204 | [MITRE ATT&CK] Command and Scripting Interpreter - T1059 | [MITRE ATT&CK] Indicator Removal on Host - T1070 | [MITRE ATT&CK] Native API - T1106 | [MITRE ATT&CK] Query Registry - T1012 | [MITRE ATT&CK] Scheduled Task - T1053 | [MITRE ATT&CK] Scripting - T1064 | [MITRE ATT&CK] Application Layer Protocol - T1071 | [MITRE ATT&CK] Command and Scripting Interpreter - T1059
Tags: China, Hospitality, Spearphishing, PowerShell, Scheduled task, Suspected-DarkHotel

Gh0stCringe RAT Being Distributed to Vulnerable Database Servers

(published: March 16, 2022)

Gh0stCringe RAT (CirenegRAT) was first detected in December 2018 being distributed via a SMB vulnerability. ASEC researchers have found that recent Gh0stCringe RAT infections were targeting database servers (Microsoft SQL and MySQL) that had account credentials vulnerable to brute force or dictionary attacks. Gh0stCringe code is based on the source code of publicly-released Gh0st RAT. For keylogging, Gh0stCringe uses Windows Polling method (GetAsyncKeyState() API), as opposed to Windows Hooking (SetWindowsHookEx() API) in Gh0st RAT. The malware can change its file size when copying itself, set the hidden or system attributes, terminate itself to disrupt analysis, and achieve persistence via registering a service and registry key.
Analyst Comment: Use long passwords with sufficient entropy and change them periodically. Maintain the latest patch for your systems. Use firewalls for database servers accessible from outside.
MITRE ATT&CK: [MITRE ATT&CK] Valid Accounts - T1078 | [MITRE ATT&CK] Brute Force - T1110 | [MITRE ATT&CK] Create or Modify System Process - T1543 | [MITRE ATT&CK] Modify Registry - T1112 | [MITRE ATT&CK] Data Staged - T1074 | [MITRE ATT&CK] Input Capture - T1056 | [MITRE ATT&CK] Obfuscated Files or Information - T1027
Tags: Gh0stCringe, CirenegRAT, Gh0st RAT, ZombieBoy, SMB, MS-SQL, MySQL, Database server, Brute force attack, Dictionary attack

Stolen Nvidia Certificates Used to Sign Malware—Here's What to Do

(published: March 15, 2022)

In March 2022, the extortionist threat group, Lapsus$ leaked Nvidia's internal data including two of Nvidia's code signing certificates. Those certificates are already being used to sign malware. Leaked signing certificates have expired (in 2014 and 2018) but Windows doesn't require a valid timestamp when signing kernel drivers if the certificate was issued before July 29, 2015.
Analyst Comment: System administrators are advised to configure Windows Defender Application Control (WDAC) policies in regards to Nvidia drivers. You can check if you have files signed with the leaked certificates in your environment: use the serial numbers 43BB437D609866286DD839E1D00309F5 and 14781bc862e8dc503a559346f5dcc518, or use Neo23x0's Yara rule.
MITRE ATT&CK: [MITRE ATT&CK] Subvert Trust Controls - T1553
Tags: Lapsus$, Nvidia, Certificate, Code signing, Windows driver, Kernel driver

What Wicked Webs We Un-Weave: Wizard Spider

(published: March 15, 2022)

Prevailion researchers detected a large-scale phishing campaign using hundreds of domains to steal credentials for Naver, a Google-like online platform in South Korea that provides email, payment, search, social, and other customer-facing services. 532 unique domains belonging to the ongoing phishing campaign targeting Naver logins were registered from August 2021 to February 2022. Prevailion didn't make a final attribution call, but notes that this Naver-targeting phishing infrastructure overlaps with Russia-based, financially-motivated threat actor group Wizard Spider, and shares similarities with some of the characteristics of Wizard Spider's associate, initial access broker Exotic Lily.
Analyst Comment: It's important to keep a watchful eye on suspicious domain registration activity related to your brand and companies from your supply chain. Anomali Targeted Threat Monitoring service can help you detect and block such suspicious domain registrations.
MITRE ATT&CK: [MITRE ATT&CK] Phishing - T1566
Tags: Naver, Wizard Spider, TrickBot, Conti ransomware, Cobalt Strike beacon, Conti, CVE-2021-40444, Phishing, South Korea, Russia

Threat Advisory: Opportunistic Cyber Criminals Take Advantage of Ukraine Invasion

(published: March 14, 2022)

Cisco Talos researchers observed scam and malware distribution actors using email lures with themes related to the military conflict in Ukraine, including humanitarian assistance and various types of fundraising. As Ukraine remains in the top news topics, this abuse is expected to increase. One of the often observed threats is a commodity remote access trojan (RAT) called Remcos that is known for its persistence via a registry run key and utilizations of a Dynamic DNS server for command and control (C2) communications.
Analyst Comment: Organizations should start proactively hunting for scam threats in their environment by building a word list to search for. Users should be trained to recognize phishing threats, and to check for possible web link spoofing by hovering the mouse over the highlighted area.
MITRE ATT&CK: [MITRE ATT&CK] Dynamic Resolution - T1568 | [MITRE ATT&CK] Modify Registry - T1112 | [MITRE ATT&CK] Phishing - T1566 | [MITRE ATT&CK] Ingress Tool Transfer - T1105
Tags: Remcos, RAT, DDNS, CVE-2017-11882, Scam, Phishing, Bitcoin, Cryptocurrency, Ukraine-Russia Conflict 2022, Ukraine

Observed Threats

Additional information regarding the threats discussed in this week's Anomali Cyber Watch can be found below:

Gamaredon Group

The Advanced Persistent Threat (APT) group "Gamaredon," is believed to be a Russia-based group that has been active since at least 2013. The group is known for conducting cyber espionage campaigns targeting the Ukrainian government, law enforcement officials, media, and military. The Lookingglass Cyber Threat Intelligence Group first reported Gamaredon in their report on a cyberespionage campaign dubbed "Operation Armageddon" in April 2015, according to Palo Alto Networks Unit 42 researchers. This led Unit 42 researchers, in February 2017, to name the group "Gamaredon Group" because they believe the group conducted Operation Armageddon.

Wizard Spider

Wizard Spider is a financially-motivated APT group operating out of Russia that has been active since 2016. Their primary activities involve the development and administration of Trickbot, Conti, Diavol, and Ryuk malware families. Wizard Spider targets large organizations for a high-ransom return. This is a technique known as big game hunting (or BGH). Their main tool, Trickbot, is a banking trojan that harvests financial credentials and Personal Identifiable Information (PII). While phishing is the main method of malware propagation, other methods such as exposed RDP services are seeing an increase in use. Known associated groups are: Grim Spider - A group that has been operating Ryuk ransomware since August 2018; reported to be a cell of Wizard Spider, and Lunar Spider - This threat group is the Eastern European-based operator and developer of the commodity banking malware called BokBot (aka IcedID). Main activities involve data theft and wire fraud.

IsaacWiper

IsaacWiper alias Lasainraw is wiper malware that enumerates the physical drive and wipes out the MBR to make the system inaccessible. On February 24, 2022, security vendor ESET observed IsaacWiper being used to target the Government of Ukraine networks. It can either be a DLL or an EXE file dropped and executed in the %programdata% or system32 location.

HermeticWiper

HermeticWiper (FoxBlade) is a sophisticated disk-wiping malware used to attack organizations in Ukraine the day prior to the launch of a Russian invasion on February 24, 2022. The malware features behavioral characteristics similar to the WhisperGate data-wiping malware first reported on January 15, 2022 by Microsoft in a destructive malware operation targeting multiple Ukraine-based organizations. HermeticWiper has two main destructive components that corrupts data and renders infected systems inoperable by damaging the Master Boot Record (MBR) and EaseUS Partition Master software.

Exploited Windows MSHTML Vulnerability (CVE-2021-40444) Was Unpatched Until September 2021

A remote code execution (RCE) vulnerability in MSHTML that affects Microsoft Windows (CVE-2021-40444) was recently reported publicly by Microsoft Threat Intelligence Center (MTIC) on 7 September, 2021. To exploit this vulnerability, a would-be attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The original exploit vector has been determined to be externally-targeted OLEObject relationship definition bearing an MHTML handler prefix pointed at an HTML file hosted on an actor infrastructure. A typical exploit for this vulnerability would use documents crafted with embedded JavaScript that downloads a cabinet file (.cab) containing a dynamic-link library (DLL) from a remote host. Once the DLL function is executed, shellcode is loaded from an attacker's remote source and into the "wabmig.exe" process (Microsoft address import tool). Observed

campaigns leveraging CVE-2021-40444 were connected to spreading various malware, including but not limited to BazaLoader, Conti ransomware, Cobalt Strike, and Trickbot.

ASSOCIATIONS (632)

URLS

hxxps://fsm-gov[.]com/

ACTIVE Confidence 85 Created 21 Mar 2022 17:25:11 iType APT URL

Tags anomali cyber watch | China | PowerShell | Scheduled task | Spear phishing | Suspected-DarkHotel | target-country:CN | target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:44.380708

hxxp://45[.]95[.]11[.]34:88/_%5BA-Z0-9%5D%7B12%7D_BZ

ACTIVE Confidence 64 Created 21 Mar 2022 17:11:08 iType APT URL

Tags anomali cyber watch | Gamaredon | InvisiMole | Operation Bleeding Bear | Primitive Bear | Russia | source-country:RU | target-country:UA | UAC-0035 | Ukraine | Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:45.916929

hxxp://45[.]95[.]11[.]34:88/_%5BA-Z0-9%5D%7B12%7D_AZ

ACTIVE Confidence 64 Created 21 Mar 2022 17:11:08 iType APT URL

Tags anomali cyber watch | Gamaredon | InvisiMole | Operation Bleeding Bear | Primitive Bear | Russia | source-country:RU | target-country:UA | UAC-0035 | Ukraine | Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

hxxp://45[.]95[.]11[.]34:3000/test

ACTIVE Confidence 64 Created 21 Mar 2022 17:11:08 iType APT URL

Tags anomali cyber watch | Gamaredon | InvisiMole | Operation Bleeding Bear | Primitive Bear | Russia | source-country:RU | target-country:UA | UAC-0035 | Ukraine | Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

hxxp://45[.]95[.]11[.]34:88/get[.]php?a=We4Qu6

ACTIVE Confidence 64 Created 21 Mar 2022 17:11:08 iType APT URL

Tags anomali cyber watch | Gamaredon | InvisiMole | Operation Bleeding Bear | Primitive Bear | Russia | source-country:RU | target-country:UA | UAC-0035 | Ukraine | Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

HASHES

c623f6ab4795a7a5300274117014a865

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:44.380708

59c6e9f8cd63893da5f4318fc6f3337d

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:44.380708

b6c77f04cef8bd327bea14ad28a8cd6a3f9c11cc

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:44.380708

163c386598e1826b0d81a93d2ca0dc615265473b66d4521c359991828b725c14

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:45.916929

965c6725acdaf2e82296302dc676cd93365288a9

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:45.916929

a251ac8cec78ac4f39fc5536996bed66c3436f8c16d377922187ea61722c71f8

ACTIVE Confidence 91 Created 21 Mar 2022 17:22:51 iType APT File Hash

Tags anomali cyber watch China PowerShell Scheduled task Spear phishing Suspected-DarkHotel target-country:CN target-industry:Hospitality

Associated Creation Date 2022-03-21T20:12:44.380708

fd72080eca622fa3d9573b43c86a770f7467f3354225118ab2634383bd7b42eb

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

dfb5a03f56769e3d1195bdfe6bb62070

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

72ed59f0d293ceede46bd69a09322f30

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

090997b4691f1a155187a181dbf54aec034eafc7b9344016867fe50da15829df

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

6b721ab9f73718c393aca2b9ad06f45b09dbfb23d105ca5872d8df7515ae14c4

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

5e06d688ac955b351c3ced0083dc7e372e447458e6604fd82ac118a6ac8e553c

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

5fb6202b8273a6a4cda73cee3f88ce1a

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

03f12262a2846ebbce989aca5cec74a7

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

4df873ea077bdbfe5389d30b5b0d0ad4a3fa663af4a4109859b61eb7f6099fc8

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

cd1a425e1ac6bc029fb4418523e43e88

ACTIVE Confidence 91 Created 21 Mar 2022 17:07:13 iType APT File Hash

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

IPS

45[.]95[.]11[.]34

ACTIVE Confidence 64 Created 21 Mar 2022 17:13:25 iType APT IP

Tags anomali cyber watch Gamaredon InvisiMole LoadEdge Operation Bleeding Bear Primitive Bear Russia source-country:RU target-country:UA UAC-0035 Ukraine Ukraine-Russia Conflict 2022

Associated Creation Date 2022-03-21T20:12:44.380708

DOMAINS

navercorpb[.]tech

ACTIVE Confidence 77 Created 20 Mar 2022 18:09:29 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navercop[.]link

ACTIVE Confidence 81 Created 20 Mar 2022 18:09:29 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navsecuritycenter[.]tech

ACTIVE Confidence 79 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

mailcontactteam[.]online

ACTIVE Confidence 64 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navercorph[.]tech

ACTIVE Confidence 90 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navoocorp[.]link

ACTIVE Confidence 57 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

nauercorpa[.]online

ACTIVE Confidence 69 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navsecorg[.]tech

ACTIVE Confidence 61 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

naveeorcorp[.]tech

ACTIVE Confidence 56 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

navmanager[.]website

ACTIVE Confidence 78 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

navercorpd[.]website

ACTIVE Confidence 83 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

naswsteam[.]site

ACTIVE Confidence 68 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

neverrcorp[.]tech

ACTIVE Confidence 59 Created 20 Mar 2022 18:09:28 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

secmanageteam[.]site

ACTIVE Confidence 73 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

naveccorp[.]link

ACTIVE Confidence 64 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

nidnavportal[.]site

ACTIVE Confidence 63 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navercorpi[.]online

ACTIVE Confidence 73 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

nauermanager[.]website

ACTIVE Confidence 78 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

nevercorp[.]online

ACTIVE Confidence 63 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

nidportalnav[.]online

ACTIVE Confidence 80 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

navcorpctr[.]online

ACTIVE Confidence 66 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navmailcenter[.]site

ACTIVE Confidence 64 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navercorpm[.]online

ACTIVE Confidence 76 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

navcorp[.]space

ACTIVE Confidence 69 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch mitre-technique:T1566 Naver Phishing Russia source-country:RU South Korea target-country:KR target-industry:IT target-region:Asia Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

corpnavcenter[.]site

ACTIVE Confidence 77 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch | mitre-technique:T1566 | Naver | Phishing | Russia | source-country:RU | South Korea | target-country:KR | target-industry:IT | target-region:Asia | Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

corpsecnav[.]site

ACTIVE Confidence 64 Created 20 Mar 2022 18:09:27 iType Phishing Domain

Tags anomali cyber watch | mitre-technique:T1566 | Naver | Phishing | Russia | source-country:RU | South Korea | target-country:KR | target-industry:IT | target-region:Asia | Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

nevercorp[.]site

ACTIVE Confidence 56 Created 20 Mar 2022 18:09:26 iType Phishing Domain

Tags anomali cyber watch | mitre-technique:T1566 | Naver | Phishing | Russia | source-country:RU | South Korea | target-country:KR | target-industry:IT | target-region:Asia | Wizard Spider

Associated Creation Date 2022-03-21T20:12:44.380708

naveroteam[.]online

ACTIVE Confidence 59 Created 20 Mar 2022 18:09:26 iType Phishing Domain

Tags anomali cyber watch | mitre-technique:T1566 | Naver | Phishing | Russia | source-country:RU | South Korea | target-country:KR | target-industry:IT | target-region:Asia | Wizard Spider

Associated Creation Date 2022-03-21T20:12:45.916929

ACTORS

Darkhotel

PUBLISHED Created 01 Mar 2017 19:17:24

Tags Darkhotel | APT | Jaku-related | APT-C-06 | DUBNIUM | Fallout Team | Karba | Luder | Nemim | Nemin | Pioneer | Shadow Crane | SIG25 | Tapaoux

Associated Creation Date 2022-03-21T20:12:57.408706

Gamaredon Group

PUBLISHED Created 23 Jun 2017 19:01:21 Tags Gamaredon Group | Operation Armagedon | Cyber espionage

Associated Creation Date 2022-03-21T20:12:57.350286

Lunar Spider

PUBLISHED Created 05 Aug 2019 14:52:17 Tags Lunar spider BokBot

Associated Creation Date 2022-03-21T20:12:57.257703

MALWARE

TrickBot

PUBLISHED Created 08 Feb 2022 19:11:41

Tags mitre-software:Trickbot detection:Trojan:Win32/Trickbot[.]GML!MTB mitre-software:TrickBot mitre-software-id:S0266

Associated Creation Date 2022-03-21T20:12:57.063925

TTP

[MITRE ATT&CK] System Information Discovery - T1082

PUBLISHED Created 25 Jun 2018 15:25:14

Tags T1082 mitre-att&ck:platform="azure" mitre-att&ck:platform="linux" mitre-att&ck:platform="aws" mitre-att&ck:platform="windows" mitre-att&ck:platform="gcp" mitre-att&ck:tactic="discovery" mitre-att&ck:permission="user" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Scheduled Task - T1053

PUBLISHED Created 25 Jun 2018 15:25:41

Tags mitre-att&ck:remote mitre-att&ck:permission="system" T1053 mitre-att&ck:effective_permssion="system" mitre-att&ck:effective_permssion="user" mitre-att&ck:platform="windows" mitre-att&ck:tactic="execution" mitre-att&ck:tactic="persistence" mitre-att&ck:effective_permssion="administrator" mitre-att&ck:tactic="privilege-escalation" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Modify Registry - T1112

PUBLISHED Created 25 Jun 2018 15:33:02

Tags mitre-att&ck:permission="system" T1112 mitre-att&ck:platform="windows" mitre-att&ck:tactic="defense-evasion" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Indicator Removal on Host - T1070

PUBLISHED Created 25 Jun 2018 15:38:11

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:platform="macos" mitre-att&ck:tactic="defense-evasion" T1070

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Data Staged - T1074

PUBLISHED Created 25 Jun 2018 15:39:06

Tags mitre-att&ck:platform="azure" mitre-att&ck:platform="linux" T1074 mitre-att&ck:platform="aws" mitre-att&ck:platform="windows" mitre-att&ck:platform="gcp" mitre-att&ck:tactic="collection" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Scripting - T1064

PUBLISHED Created 25 Jun 2018 15:39:32

Tags T1064 mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="execution" mitre-att&ck:tactic="defense-evasion" mitre-att&ck:permission="user" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] User Execution - T1204

PUBLISHED Created 25 Jun 2018 15:40:20

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="execution" mitre-att&ck:permission="user" mitre-att&ck:platform="macos" T1204

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Brute Force - T1110

PUBLISHED Created 25 Jun 2018 15:44:15

Tags mitre-att&ck:tactic="credential-access" mitre-att&ck:platform="azure" mitre-att&ck:platform="linux" T1110 mitre-att&ck:platform="azure ad" mitre-att&ck:platform="saas" mitre-att&ck:platform="windows" mitre-att&ck:platform="gcp" mitre-att&ck:permission="user" mitre-att&ck:platform="macos" mitre-att&ck:platform="aws" mitre-att&ck:platform="office 365"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Valid Accounts - T1078

PUBLISHED Created 25 Jun 2018 15:44:59

Tags mitre-att&ck:platform="saas" mitre-att&ck:platform="azure ad" mitre-att&ck:platform="azure" mitre-att&ck:platform="linux" mitre-att&ck:effective_permssion="user" T1078 mitre-att&ck:platform="aws" mitre-att&ck:tactic="initial-access" mitre-att&ck:platform="windows" mitre-att&ck:platform="gcp" mitre-att&ck:tactic="persistence" mitre-att&ck:tactic="defense-evasion" mitre-att&ck:tactic="privilege-escalation" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator" mitre-att&ck:platform="macos" mitre-att&ck:effective_permssion="administrator" mitre-att&ck:platform="office 365"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Obfuscated Files or Information - T1027

PUBLISHED Created 25 Jun 2018 15:45:47

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:platform="macos" mitre-att&ck:tactic="defense-evasion" T1027

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Input Capture - T1056

PUBLISHED Created 25 Jun 2018 15:47:19

Tags mitre-att&ck:tactic="credential-access" mitre-att&ck:permission="system" mitre-att&ck:permission="root" mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" T1056 mitre-att&ck:tactic="collection" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Query Registry - T1012

PUBLISHED Created 25 Jun 2018 15:49:01

Tags mitre-att&ck:permission="system" T1012 mitre-att&ck:platform="windows" mitre-att&ck:tactic="discovery" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Data Encrypted for Impact - T1486

PUBLISHED Created 24 Jun 2019 10:03:49

Tags mitre-att&ck:permission="system" mitre-att&ck:tactic="impact" mitre-att&ck:permission="root" mitre-att&ck:platform="linux" T1486 mitre-att&ck:platform="windows" mitre-att&ck:permission="user" mitre-att&ck:permission="administrator" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Data Destruction - T1485

PUBLISHED Created 24 Jun 2019 10:05:47

Tags mitre-att&ck:permission="system" mitre-att&ck:tactic="impact" mitre-att&ck:permission="root" mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" T1485 mitre-att&ck:permission="user" mitre-att&ck:permission="administrator" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Ingress Tool Transfer - T1105

PUBLISHED Created 09 Jul 2020 21:01:04

Tags T1105 mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="command-and-control" mitre-att&ck:permission="user" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Create or Modify System Process - T1543

PUBLISHED Created 10 Jul 2020 20:55:20

Tags mitre-att&ck:platform="linux" T1543 mitre-att&ck:platform="windows" mitre-att&ck:tactic="persistence" mitre-att&ck:tactic="privilege-escalation" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Protocol Tunneling - T1572

PUBLISHED Created 10 Jul 2020 21:05:30

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:platform="macos" T1572 mitre-att&ck:tactic="command-and-control"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Application Layer Protocol - T1071

PUBLISHED Created 10 Jul 2020 21:06:09

Tags T1071 mitre-att&ck:network mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="command-and-control" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Dynamic Resolution - T1568

PUBLISHED Created 10 Jul 2020 21:06:28

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="command-and-control" mitre-att&ck:permission="user" mitre-att&ck:platform="macos" T1568

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Phishing - T1566

PUBLISHED Created 10 Jul 2020 21:08:03

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="saas" mitre-att&ck:tactic="initial-access" mitre-att&ck:platform="windows" T1566 mitre-att&ck:platform="macos" mitre-att&ck:platform="office 365"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Subvert Trust Controls - T1553

PUBLISHED Created 12 Jul 2020 21:15:48

Tags mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:platform="macos" mitre-att&ck:tactic="defense-evasion" T1553

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Native API - T1106

PUBLISHED Created 13 Jul 2020 20:55:55

Tags T1106 mitre-att&ck:platform="linux" mitre-att&ck:platform="windows" mitre-att&ck:tactic="execution" mitre-att&ck:permission="user" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

[MITRE ATT&CK] Command and Scripting Interpreter - T1059

PUBLISHED Created 14 Jul 2020 20:55:53

Tags mitre-att&ck:platform="linux" T1059 mitre-att&ck:platform="windows" mitre-att&ck:tactic="execution" mitre-att&ck:permission="user" mitre-att&ck:platform="macos"

Associated Creation Date 2022-03-21T20:12:47.917577

HISTORY

Updated Report	21 Mar 2022 20:49:47
Published Report	21 Mar 2022 20:42:27
Updated Report	21 Mar 2022 20:41:15
Updated Report	21 Mar 2022 20:39:44
Updated Report	21 Mar 2022 20:18:08
Association Added	21 Mar 2022 20:12:47
Updated Intelligence	21 Mar 2022 20:12:46

Updated Intelligence	21 Mar 2022 20:12:45
Created Report	21 Mar 2022 20:12:44

COMMENTS