context

AVIVORE - An overview of Tools, Techniques and Procedures

contextis.com
E info@contextis.com
T +44 (0)207 537 7515

context

AVIVORE

An overview of Tools, Techniques and Procedures

AVIVORE - An overview of Tools, Techniques and Procedures

Earlier this month, Context released a blog post on 'AVIVORE' - a new threat actor responsible for a series of linked intrusions against Aerospace, Defence and related industries including Automotive, Consultancy, Engineering, Civil Nuclear, and Space and Satellites. Following this initial release other entities have publicly shared additional information and indicators of compromise associated with the intrusion.
Context is now able to release further technical detail on the Tactics, Techniques and Procedures (TTPs) observed in this campaign, including Indicators of Compromise.

30 Second Campaign Recap and Adversary Overview

— A sophisticated nation state adversary succeeded in stealing data from several multinational defence firms (Primes) despite their significant security teams.

— The adversary's entry point into Primes was via smaller engineering or consultancy firms that sat within their supply and value chains (Secondaries).

— Secondaries are typically high-tech engineering suppliers; organisations that are critical to current and legacy platforms, and where recovery can have a significant business impact.

— AVIVORE are not using malicious software; their tradecraft is "living off the land" which makes detection extremely difficult.

— Custom tools deployed by AVIVORE contained functionality to hijack web browser based information and related authentication/session information.

— Since summer 2018, Context has worked closely with victims, security organisations, and law enforcement agencies across Europe to reduce impact and prevent further compromises.

— AVIVORE is extremely capable and highly-likely to try to replicate the success of this campaign; likely future targets are high-tech service providers for intellectual property theft and access enablement.

avivore (noun) - a specialised predator of birds

Characteristic	Description
Class	Nation State Endorsed Adversary
Active Since	October 2015, although forensics evidence in some victim environments suggests attacker activity aligned with AVIVORE TTPs taking place as long ago as mid-2013
Country of Origin	Suspected to be China, based on a number of factors including actor operating hours (+0800), infrastructure used, keyboard layout and language artefacts.
Primary Language	Most likely Chinese, though operators have also demonstrated proficiency in English and (at a minimum) basic understanding of French and German.
Motivation	*Primary* - technical espionage, related to engineering, R&D and innovation across a number of sectors *Secondary* - access enablement; maintaining persistent, covert access into the defence/engineering supply chain.
Observed	*Regions* - Americas, Asia, Europe *Verticals* - Aerospace, Astronautics, Automotive, Defence, Engineering Consultancy, IT Services, Nuclear, Satellite Technology

AVIVORE TTPs

To aid in development of playbooks and ongoing adversary tracking, Context analysts mapped all of the techniques observed across AVIVORE intrusions to the MITRE ATT&CK™ framework.

Initial Access

T1133 External Remote Services
T1195 Supply Chain Compromise
T1199 Trusted Relationship
T1078 Valid Accounts

context

AVIVORE

An overview of Tools, Techniques and Procedures

Attack Overview

AVIVORE exploited the interconnected relationship between organisations to conduct activity across multiple business units or geographical locales; a technique referred to as "Island Hopping". Affected Secondaries frequently maintained direct network connectivity - via Virtual Private Networks (VPNs) or other remote working solutions - into multiple Primes. This enabled AVIVORE to evade critical controls and bypass the (generally well-defended) perimeters of the Primes.

Context assesses with moderate confidence that the objective of the campaign was intellectual property theft from victim organisations. Information and assets sought by the actor to enable these intrusions have included:

— Domain Administrator and privileged service accounts, as well as accounts belonging to senior members of IT and Information Security teams, or Managed Service Providers.

— Internal network diagrams, guides for services such as customer VPNs and other information related to network architecture, configuration, and security operations functions.

— Public Key Infrastructure information, associated certificates, and any supporting information which may enable the adversary to conduct certificate-based authentication or otherwise manipulate network trust.

— Access to laptops and workstations belonging to senior technical staff members.

In addition to Aerospace and Defence engineering victims, Context has seen AVIVORE target systems or assets related to a number of other verticals:

— Automotive (theft of VPN configuration information)

— Consultancy (compromise for onward island hopping)

— Energy/Nuclear (enumeration of remote connectivity assets)

— Space and Satellite Technology (enumeration of remote connectivity assets)

Initial Access and Persistence

The majority of activity investigated by Context has taken place since Jan/Feb 2018. However, there were artefacts present in some victim environments which indicate that AVIVORE (or a related group) maintained persistent access since at least October 2015. The initial access vector into the Secondaries is unconfirmed, although compromise of external facing infrastructure is likely.

Multiple instances of the PlugX Remote Access Trojan were discovered on compromised hosts within Secondaries' environments. Evidence suggests these implants were deployed between October 2015 and October 2016. The PlugX binaries were located in two locations and were designed to look like components of Anti-virus software:

```
c:\programdata\esetoem\
c:\programdata\mcafeeoem\
```

The samples identified used a legitimate signed McAfee binary (`mc.exe – 884d46c01c762ad6ddd2759fd921bf71`) to side-load a PlugX DLL loader (`McUtil.dll – b536576a7a8ac362b00169f77fa7cd45`), which in turn was used to decrypt the implant payload (`mc.cp – various hashes`) and inject it into a running svchost process.

Execution

T1059 Command-Line Interface
T1061 Graphical User Interface
T1086 PowerShell
T1053 Scheduled Task
T1064 Scripting
T1035 Service Execution
T1218 Signed Binary Proxy Execution
T1047 Windows Management Instrumentation

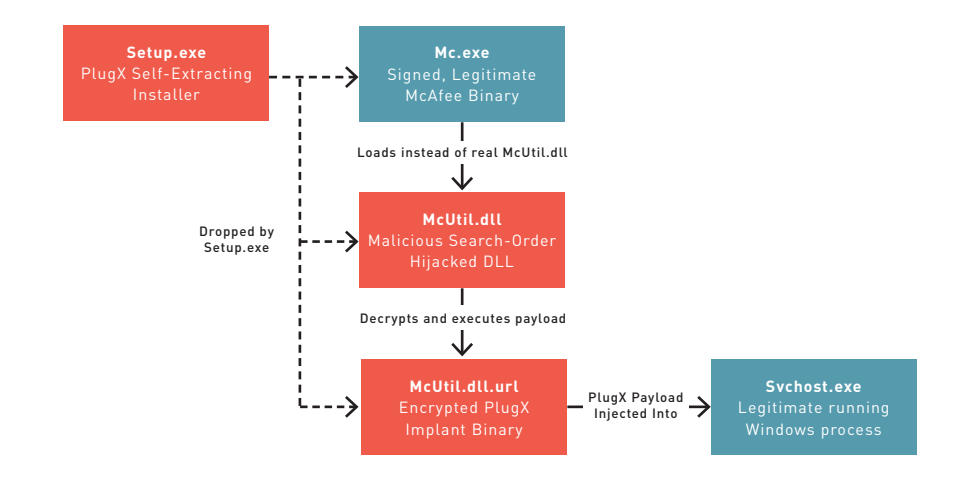

Figure 1 - PlugX search-order hijacking example using McAffee OEM Module

Although direct interaction with these implants was not observed during the investigation, Context assess with low-moderate confidence that they may be associated with the AVIVORE intrusions. Evidence indicates that some of the implants were patched in-memory, with modified configuration blocks. These were injected post-execution to provide new Command & Control (C2) domains during times AVIVORE operators were known to be active inside victim environments. Patching of the C2 infrastructure on a live implant suggests AVIVORE have significant familiarity with the PlugX family; potentially with access to source code enabling them to determine the correct technique to accomplish this.

```
Service Disp                    McAfeeOEM
Lateral movement UDP port       1357
Screenshots params              10 sec / Zoom 50 / 16 bits / Quality 50 / Keep 3 days
C&C Address                     home.GRAYTAGS.COM:80 (UDP(6))
                                zone.GRAYTAGS.COM:53 (DNS(5))
                                zone.GRAYTAGS.COM:80 (ICMP(7))
                                home.GRAYTAGS.COM:80 (TCP(3))

Service Disp                    McAfeeOEM
Lateral movement UDP port       1357
Screenshots params              10 sec / Zoom 50 / 16 bits / Quality 50 / Keep 3 days
C&C Address                     can.COPAININFO.COM:80 (UDP(6))
                                help.COPAININFO.COM:53 (DNS(5))
                                help.COPAININFO.COM:80 (ICMP(7))
                                can.COPAININFO.COM:80 (TCP(3))
```

Figure 2 - Statically extracted PlugX configuration (top) versus memory capture of same PlugX infection (bottom), showing patched C2 addresses

Discovery, Privilege Escalation and Execution

Once inside victim networks AVIVORE showed themselves to be highly capable; adept at both "living-off-the-land" (masquerading as legitimate users) and in their operational security awareness.

During the early stages of intrusions, AVIVORE utilised in-built system commands such as 'net', 'ver' and 'whoami' to enumerate accounts, domain trusts and system configuration information. Context also observed them browsing through file shares on victim systems as well as online storage services such as OneDrive. Patterns of browsing indicated an interest in documentation relating to network diagrams, collaborative projects, and remote service configuration. The adversary demonstrated a detailed knowledge of critical individuals associated with IT administration and special projects, and was able to successfully mirror working times and patterns of these legitimate users in order to avoid arousing suspicions.

Persistence

T1098	Account Manipulation
T1136	Create Account
T1038	DLL Search Order Hijacking
T1133	External Remote Services
T1031	Modify Existing Service
T1050	New Service
T1108	Redundant Access
T1060	Registry Run Keys / Startup Folder
T1053	Scheduled Task
T1078	Valid Accounts

On a number of occasions, AVIVORE introduced network scanning and certificate management tools, notably 'SoftPerfect Network Scanner' and 'CertMig', into victim environments for network discovery and facilitation of onward intrusion. In addition to this, evidence supports that the attackers forced the caching of plaintext credentials on crucial systems such as Domain Controllers by modifying the Windows Authentication Digest (WDigest) UseLogonCredential registry key[1]. This was followed by dumping the running memory of the Local Security Authority Subsystem Service (lsass) using Windows SysInternals ProcDump, MimiKatz and Windows Task Manager; ultimately providing the attackers with further credentials for onwards compromise.

Tools were typically renamed to imitate Windows binaries associated with compatibility and patching and staged in associated directories:

Legitimate Binary	Attacker Tool Rename	Typical Location
Acres.dll	Acres.exe	'C:\PerfLogs\' 'C:\Windows\AppPatch\Custom\'
Acres64.dll	Acres64.exe	
AcWinRT.dll	AcWinRT.exe	'C:\PerfLogs\Admin\'
Apihex.dll	ApiHex.exe	'C:\PerfLogs\Admin\' 'C:\Windows\AppPatch\'
Apihex64.dll	Apihex64.exe	

AVIVORE relied on a combination of remote and local scheduled tasks to execute generically named scripts with 'SYSTEM' level privileges. Across investigations, Context recorded the adversary using PowerShell, VBS and batch scripts running out of their preferred staging locations. The below example of a remote scheduled task creation was seen in multiple victim environments. Such tasks would include a scheduled delete set for a few minutes after successful execution.

```
schtasks  /create /S <REMOTEHOST> /U <ADMINUSER> /P <PASSWORD> /tn
System /ru system /f /tr c:\windows\AppPatch\clr.bat /sc once /st
03:05
```

Figure 3- Remote task scheduling as SYSTEM

Lateral Movement, Defence Evasion and Collection

AVIVORE made extensive use of infrastructure that provided interconnectivity between victims; they employed different routes to issue tasking and to stage data for exfiltration. Lateral movement was accomplished primarily through Remote Desktop Protocol (RDP) using compromised credentials, Net commands, modified WMIExec[2] VBScripts, and use of SMB and NetBIOS when scheduling remote execution of their tools. In order to avoid identification and hinder investigation, Context observed AVIVORE using multiple RDP sessions between geographically-disparate locations, often initiating sessions within sessions.

Privilege Escalation

T1134 Access Token Manipulation
T1038 DLL Search Order Hijacking
T1068 Exploitation for Privilege Escalation
T1179 Hooking
T1050 New Service
T1055 Process Injection
T1053 Scheduled Task
T1078 Valid Accounts

[1] https://blogs.technet.microsoft.com/askpfeplat/2016/04/18/the-importance-of-kb2871997-and-kb2928120-for-credential-protection/

[2] https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

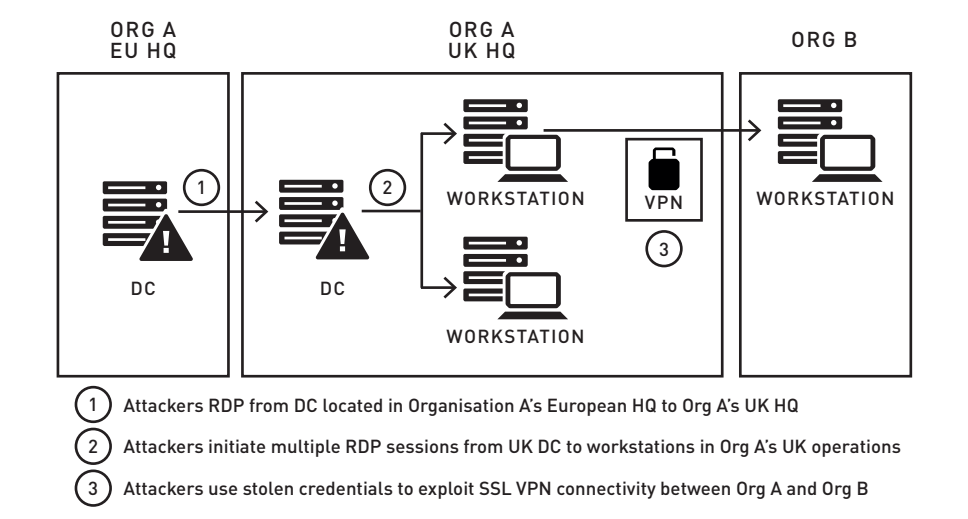

Figure 4 - Attacker Lateral Movement across Geographical and Organisational Boundaries

AVIVORE facilitated and obfuscated their RDP sessions by modifying local firewall rules on hosts; the native Windows "netsh" command was used to configure proxying of RDP and SSL VPN traffic over non-standard ports, particularly TCP/53 and TCP/1443. This allowed them to bypass network monitoring, security appliances or other limitations designed to restrict RDP between hosts in victim environments.

```
netsh  interface portproxy add v4tov4 listenport=53
connectaddress=127.0.0.1 connectport=3389
```

Figure 5-Configuring proxy of RDP traffic using 'netsh'

The same technique was also used to establish "proxy" or "bouncer" hosts, which are designed to route traffic originating from one host on a particular port, to another host on a different port; effectively creating bastion hosts between segregated/separated networks.

AVIVORE displayed an exceptional level of forensic awareness; taking actions designed specifically to deny investigators forensic evidence into many of their techniques. Most notably, Context observed the adversary using the Windows Registry Editor (RegEdit.exe) to remove the artefacts associated with RDP sessions they had established between hosts. This was often the first action taken once they had connected to the target machine. Similarly, AVIVORE were observed clearing artefacts of failed logons and established network connections from the Windows event logs of compromised hosts, and removing entries from hosts' antivirus logs.

Another element of AVIVORE's defence evasion capabilities included a custom browser injection tool designed to allow extraction of content from, or injection of content into, active web browsing sessions. Artefacts suggest that the tool was created during an ongoing intrusion, its creation correlating with a configuration change made to remote access controls in one victim organisation. The specific application of the tool appears to enable interaction with remotely-accessible virtual application environments post-authentication.

The majority of collection activity observed by Context was focused on enablement of onward intrusions into third party organisations; the theft of machine certificates, VPN configuration files and network architecture diagrams enabled AVIVORE to establish their own direct inbound connections into victim environments by impersonating legitimate users. This activity was automated via scripts and scheduled tasks and captured data was transferred to beachhead hosts, often those same bastion hosts that sat between different networks that were used to proxy attacker network connections.

Defence Evasion

T1088	Bypass User Account Control
T1116	Code Signing
T1038	DLL Search Order Hijacking
T1140	Deobfuscate/Decode Files or Information
T1089	Disabling Security Tools
T1107	File Deletion
T1070	Indicator Removal on Host
T1036	Masquerading
T1112	Modify Registry
T1126	Network Share Connection Removal
T1027	Obfuscated Files or Information
T1055	Process Injection
T1108	Redundant Access
T1064	Scripting
T1218	Signed Binary Proxy Execution
T1045	Software Packing
T1099	Timestomp
T1078	Valid Accounts
T1102	Web Service

context

AVIVORE

An overview of Tools, Techniques and Procedures

C2 and Exfiltration

PlugX C2 domains aside, network infrastructure employed by AVIVORE primarily consisted of commercial VPNs located in Singapore and Japan and use of Tor. It is likely that AVIVORE selected these VPN services because, in at least one instance, they were used by legitimate employees of the victim organisations; making it more likely for these to be a permitted source for inbound remote connections.

Both Tor and commercial VPN solutions were used by AVIVORE to connect into victims' external-facing FTP or SFTP servers for which they had stolen credentials during earlier stages of their intrusions. Frequently these S/FTP servers were part of the victim organisation's 'Shadow IT' infrastructure – unmonitored, legacy and/or business edge-case hosts that were often believed to have been decommissioned. AVIVORE utilised a combination of SMB and RPC to transport and stage files across client infrastructure, leveraging stolen credentials to access the IPC$[3] share. Prior to exfiltration, data would be chunked, encrypted and compressed using command-line tools, most notably rar.exe. Across several intrusions Context observed AVIVORE using common passwords to secure these archives.

Adversay Attribution

Context categorise AVIVORE as a previously unknown and untracked nation-state level adversary. The operators' working hours appear to correlate to a time zone of UTC +8, and keyboard layout settings and language artefacts suggest the attackers are of Chinese-origin. The primary objective for their intrusions is believed to be espionage, as well as access enablement through supply chain partners.

Recent reporting into incidents affecting Aerospace and Defence Primes has speculated that either APT10 or JSSD (Jiangsu Province Ministry of State Security) may be responsible for this activity[4]. Whilst certain similarities between these adversaries' campaigns and those investigated by Context exist, the Tactics, Techniques and Procedures (TTPs), infrastructure and tooling observed do not align with Context's ongoing tracking of these other operators.

AVIVORE are judged by Context to be a high-severity threat to organisations operating in sectors beyond aerospace and defence. During our investigations AVIVORE expressed an interest in technical assets linked to service sectors including energy infrastructure, automotive/transportation (particularly in reference to renewable technology) and innovative industrial processes. Whilst this may be an artefact of the sheer diversity of the civil and military aerospace supply-chain, broader targeting of these industries cannot be discounted; these verticals align closely with Chinese state interests, which AVIVORE are believed to perform technical espionage and access enablement to support.

Credential Access

T1098 Account Manipulation
T1110 Brute Force
T1003 Credential Dumping
T1081 Credentials in Files
T1214 Credentials in Registry
T1040 Network Sniffing

[3] https://support.microsoft.com/en-gb/help/3034016/ipc-share-and-null-session-behavior-in-windows

[4] https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

context

AVIVORE

An overview of Tools, Techniques and Procedures

Mitigations

Based on the information and assets sought by AVIVORE, Context assesses with moderate confidence that the objective of the recent campaign was intellectual property theft from victim organisations, as well as access enablement through supply chain partners. Although defence against advanced nation-state level actors can be challenging, Context recommend the following mitigations to disrupt future AVIVORE activity:

— Impose access limitations on supplier connections over VPNs, such as preventing their use outside of the supplier's business hours or from IP addresses and locations other than those pre-agreed, and restrict access only to data and assets they require to perform their actions.

— Ensure that security measures, such as multifactor authentication and enhanced auditing/logging are deployed to hosts and services into which suppliers are required to connect, in order to prevent or support the investigation of any suspicious user behaviour.

— Ensure that external remote access services implement appropriate log retention. Logs should contain enough information on the sources of inbound connections to enable identification of anomalies, such as concurrent log-ins with impossible geography.

— Ensure that credentials for highly privileged accounts and remote services are stored securely, and their use is appropriately monitored. Hosts such as domain controllers, sensitive file shares and Public Key Infrastructure servers, should also be subject to particular additional scrutiny and monitoring.

— Where possible, applications, documentation and technical information related to network infrastructure and configuration of remote access services should be made available only to engineers, IT support staff and other individuals with legitimate business need.

Indicators of Compromise

Due to AVIVORE's extensive use of publicly-available tooling as well as legitimate Windows locations for staging of capability, a number of the indicators provided below may be prone to false positive hits. It is advised that these indicators are used in conjunction with other artefacts such as file names and paths to limit the likelihood of incidental hits.

Discovery

T1087	Account Discovery
T1217	Browser Bookmark Discovery
T1083	File and Directory Discovery
T1046	Network Service Scanning
T1135	Network Share Discovery
T1069	Permission Groups Discovery
T1057	Process Discovery
T1018	Remote System Discovery
T1082	System Information Discovery
T1016	System Network Configuration Discovery
T1049	System Network Connections Discovery
T1007	System Service Discovery
T1124	System Time Discovery

E info@contextis.com
T +44 (0)207 537 7515

context

AVIVORE

An overview of Tools, Techniques and Procedures

Indicator	Type	Filename	Comment
884d46c01c762ad6ddd2759fd921bf71 3124fcb79da0bdf9d0d1995e37b06f 7929d83c1c4b60e38c104743be71170efe	MD5 SHA256	mc.exe	Legitimate, signed McAfee binary used to side-load PlugX implants.
b536576a7a8ac362b00169f77fa7cd45 a28964ccf4f6e177b3972290948c1c3b03 0dbd1df8b496f9eccc275d1bd19049	MD5 SHA256	McUtil.dll	PlugX loader DLL, used to decrypt and execute the PlugX payload.
cffeea3e795fa71032a7668e33fb1e5a 76c613289ef2758f12b7d5bb8746eeae579 d69e46388b76c20c88de72f8583c2	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
e075376642f1e3fefe35ea3969135fa1 6af27beab13eb61b96a2debbbe73099 e09489ee9832965fbfed946bb5dfc93f3	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
a2ad7148c6cdba9003cf0aeecb6266d5 6dbc88b41e7a013e08c2595fa6f43e65cf 18ee3e286219caaffa7aa219193663	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
3d1ec6a9e664532ef0f4e0777e6e2e2b dd8642ec60e1762747c0d646eff5c80b58db 9325ca00812435a2e5b2097acf54	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
051c5668fe829aecb0361938165bfb87 c07a6eeb35bd274b216e9f246e3f1d4f766 fd3fb2a418e407ce5454ec6d7a47f	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
b9c7f14680597dfc756ebf579a0a3876 141a37efa5447bc48a98b3e49378b3f215 bad4c0c400df22b6a33782ac6f6fae	MD5 SHA256	mc.cp	Encrypted PlugX implant payload
6a09bc6c19c4236c0bd8a01953371a29 05732e84de58a3cc142535431b3aa04efbe 034cc96e837f93c360a6387d8faad	MD5 SHA256	acres.exe apihex64.exe	SysInternals ProcDump version (32-bit)
a92669ec8852230a10256ac23bbf4489 16f413862efda3aba631d8a7ae2bfff6 d84acd9f454a7adaa518c7a8a6f375a5	MD5 SHA256	acres64.exe apihex64.exe apihex6464.exe	SysInternals ProcDump version (64-bit)
4f8c16d010febdd10d9617413af8def1 f7c9bdc5ede32642430dbd6f7951791f 455c1a4138aded574ec1535932bbf5b2	MD5 SHA256	apihex64.exe	CertMig certificate export tool
286e94426f27755fa52786b3f0a2c06a 515e8d63526d39b993dde01fb313b8f32f da374ac5435bedebd30e73321038ec	MD5 SHA256	AcWinRT.exe netscan.exe	NetScan 5.1.4 port/protocol scanning tool
609c38e389fda3ee7c5e81d7ac857dc9 a87e808bdd92726c4d1f1eb60167c870 d3eb073dafb8d1fe4c21834c28af45cd	MD5 SHA256	w.vbs	Slightly modified WMIExec.vbs lateral movement/ remote command execution script

Lateral Movement

T1210 Exploitation of Remote Services
T1075 Pass the Hash
T1076 Remote Desktop Protocol
T1105 Remote File Copy
T1021 Remote Services
T1077 Windows Admin Shares

Collection

T1119 Automated Collection
T1115 Clipboard Data
T1074 Data Staged
T1213 Data from Information Repositories
T1005 Data from Local System
T1039 Data from Network Shared Drive
T1056 Input Capture
T1185 Man in the Browser
T1113 Screen Capture

context

AVIVORE

An overview of Tools, Techniques and Procedures

Filepath	Comment
c:\iperf-2.0.5-3-win32\	Attacker staging location
c:\perflogs\	Attacker staging location
c:\perflogs\admin	Attacker staging location
c:\programdata\esetoem\	PlugX installation location
c:\programdata\mcafeeoem\	PlugX installation location
c:\temp\	Attacker staging location
c:\temp\gen_py\	Attacker staging location
c:\windows\AppPatch	Attacker staging location
c:\windows\AppPatch\custom	Attacker staging location

Indicator	Type	Comment
shop.addailymotion.com	Domain	PlugX command and control (C2) domain
uick.addailymotion.com	Domain	PlugX command and control (C2) domain
ama.chiamate6590.com	Domain	PlugX command and control (C2) domain
bbq.chiamate6590.com	Domain	PlugX command and control (C2) domain
can.copaininfo.com	Domain	PlugX command and control (C2) domain
help.copaininfo.com	Domain	PlugX command and control (C2) domain
as.gestione6781.com	Domain	PlugX command and control (C2) domain
bae.gestione6781.com	Domain	PlugX command and control (C2) domain
one.gestione6781.com	Domain	PlugX command and control (C2) domain
home.graytags.com	Domain	PlugX command and control (C2) domain
mx.graytags.com	Domain	PlugX command and control (C2) domain
zone.graytags.com	Domain	PlugX command and control (C2) domain
45.56.153.0/24	IP Address Range	VPN Consumer Network Singapore IP address range, used by actors for interactive connections into victim environments
64.64.108.0/24	IP Address Range	ExpressVPN Japan IP address range, used by actor for interactive connections into victim environments.

Command and Control

T1043 Commonly Used Port
T1090 Connection Proxy
T1094 Custom Command and Control Protocol
T1188 Multi-hop Proxy
T1026 Multiband Communication
T1105 Remote File Copy
T1071 Standard Application Layer Protocol
T1095 Standard Non-Application Layer Protocol

Exfiltration

T1002 Data Compressed
T1048 Exfiltration Over Alternative Protocol

contextis.com
E info@contextis.com
T +44 (0)207 537 7515