Agrius, Pink Sandstorm, AMERICIUM, Agonizing Serpens, BlackShadow, Group G1030

Archived: 2026-04-05 13:44:03 UTC

Enterprise T1583 Acquire Infrastructure

Agrius typically uses commercial VPN services for anonymizing last-hop traffic to victim networks, such as ProtonVPN.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Agrius used 7zip to archive extracted data in preparation for exfiltration.[5]

Enterprise T1119 Automated Collection

Agrius used a custom tool, `sql.net4.exe`, to query SQL databases and then identify and extract personally identifiable information.[5]

Enterprise T1110 Brute Force

Agrius engaged in various brute forcing activities via SMB in victim environments.[5]

.003 Password Spraying

Agrius engaged in password spraying via SMB in victim environments.[5]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Agrius uses ASPXSpy web shells to enable follow-on command execution via `cmd.exe`.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Agrius has deployed IPsec Helper malware post-exploitation and registered it as a service for persistence.[1]

Enterprise T1005 Data from Local System

Agrius gathered data from database and other critical servers in victim environments, then used wiping mechanisms as an anti-analysis and anti-forensics mechanism.[5]

Enterprise T1074 .001 Data Staged: Local Data Staging

Agrius has used the folder, `C:\windows\temp\s\`, to stage data for exfiltration.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

Agrius has deployed base64-encoded variants of ASPXSpy to evade detection.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Agrius exfiltrated staged data using tools such as Putty and WinSCP, communicating with command and control servers.[5]

Enterprise T1190 Exploit Public-Facing Application

Agrius exploits public-facing applications for initial access to victim environments. Examples include widespread attempts to exploit CVE-2018-13379 in FortiOS devices and SQL injection activity.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Agrius used several mechanisms to try to disable security tools. Agrius attempted to modify EDR-related services to disable auto-start on system reboot. Agrius used a publicly available driver, `GMER64.sys` typically used for anti-rootkit functionality, to selectively stop and remove security software processes.[5]

Enterprise T1570 Lateral Tool Transfer

Agrius downloaded some payloads for follow-on execution from legitimate filesharing services such as `ufile.io` and `easyupload.io`.[2]

Enterprise T1036 Masquerading

Agrius used the Plink tool for tunneling and connections to remote machines, renaming it `systems.exe` in some instances.[5]

Enterprise T1046 Network Service Discovery

Agrius used the open-source port scanner `WinEggDrop` to perform detailed scans of hosts of interest in victim networks.[5]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Agrius used tools such as Mimikatz to dump LSASS memory to capture credentials in victim environments.[5]

.002 OS Credential Dumping: Security Account Manager

Agrius dumped the SAM file on victim machines to capture credentials.[5]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Agrius tunnels RDP traffic through deployed web shells to access victim environments via compromised accounts.[1] Agrius used the Plink tool to tunnel RDP connections for remote access and lateral movement in victim environments.[5]

Enterprise T1018 Remote System Discovery

Agrius used the tool NBTscan to scan for remote, accessible hosts in victim environments.[5]

Enterprise T1505 .003 Server Software Component: Web Shell

Agrius typically deploys a variant of the ASPXSpy web shell following initial access via exploitation.[1]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

Agrius attempted to acquire valid credentials for victim environments through various means to enable follow-on lateral movement.[5]
