NETWITNESS

FIRSTWATCH

SECURITY BULLETIN

Guidance and Recommendations
from Operation Endgame

Guidance and Recommendations from Operation Endgame

A recent operation coordinated by Europol targeted several significant malware droppers, including IcedID, SystemBC, Pikabot, Smoke Loader, Bumblebee, and Trickbot. These malware families are known for their sophisticated techniques and widespread use in cybercriminal activities. The operation, named 'Endgame,' took place between May 27 and 29, 2024, and resulted in the arrest of high-value targets and the dismantling of criminal infrastructure.

France, Germany, and the Netherlands led the strategic operation, supported by Eurojust and actively involved countries such as Denmark, the UK, and the US. This operation marked the most extensive effort against botnets to date, with additional support provided by Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland, Ukraine, and vital private partners like Bitdefender, Cryptolaemus, and Shadowserver.

The 'Endgame' operation led to significant financial repercussions for the cybercriminals. Four arrests, 16 location searches, the disruption or takedown of over 100 servers, and control over 2000 domains were the tangible results. Notably, a primary suspect was discovered to have earned at least EUR 69 million in cryptocurrency by renting out criminal infrastructure for ransomware deployment, leading to legal actions for asset seizure.

Furthermore, a 28-year-old Russian man in Kyiv was arrested by the Ukraine cyber police for working with Conti and LockBit ransomware operations. This individual specialized in developing custom crypters to make ransomware payloads undetectable by popular antivirus products.

Despite the significant success of the 'Endgame' operation, Europol is committed to continuing the fight against botnets and cybercrime. The operation not only showcased the importance of cross-border and public-private partnerships in countering cybercriminal infrastructure but also served as a powerful deterrent to

Guidance and Recommendations from Operation Endgame (cont.)

cybercriminal activities.

NetWitness Takeaways:

NetWitness Live has several pieces of detection logic that can help identify behaviors associated with Operation Endgame malware families. These include:

- Autorun Invalid Signature Windows Directory
- Autorun Key Contains Non-Printable Characters
- Autorun Unsigned BootExecute Registry Startup Method
- Autorun Unsigned Explorer Registry Startup Method
- Autorun Unsigned Hidden Only Executable In Directory
- Autorun Unsigned In AppDataLocal Directory
- Autorun Unsigned In AppDataRoaming Directory
- Autorun Unsigned In ProgramData Directory
- Autorun Unsigned LogonType Registry Startup Method
- Autorun Unsigned Winlogon Helper DLL
- Cobalt Strike Service Installations in Registry
- Cobalt Strike Getsystem Service Detected
- Using Query Utility
- Scheduled Tasks via schtasks.exe (Logs)
- Tasks In ProgramData Directory
- Floating Module In Browser Process
- Modifies Image File Execution for Persistence
- Modifies Run Key
- Modifies Startup Folder Location
- Modifies Winlogon DLL for Persistence
- MS Office File Launches Regsvr32 Child Process
- Potential Dynamic Linker Hijack using LD Preload
- Remote Thread into LSASS
- Runs Powershell With Hidden Window
- Runs Tasks Management Tool
- Scheduled Tasks via schtasks.exe (Endpoint)
- Unsigned File Creates Run Key
- Unsigned Hidden Windows File Creates Remote Thread
- Unsigned Windows File Creates Remote Thread
- Floating Module
- Floating Module And Hooking

Guidance and Recommendations for Bumblebee

***********The above list should be combined with the malware-specific information provided below to detect suspicious activity using NetWitness.*********

Bumblebee

Bumblebee is a malware loader used by several threat groups, including the defunct Conti ransomware gang and Exotic Lily. It is typically delivered to victim systems using phishing emails containing links to malicious OneDrive URLs or macro-enabled attachments. Cobalt Strike payloads typically follow many Bumblebee infections.

NetWitness Logic:

- Bumblebee - Known Execution Attempt

Hunting Queries:

- device.type = 'nwendpoint' && category = 'process event' && action = 'createremotethread' && filename.src = 'wabmig.exe','wab.exe','imagingdevices.exe' && filename.dst = 'rundll32.exe'
- device.type = 'nwendpoint' && category = 'file event' && action = 'renametoexecutable', 'writetoexecutable' && filename.src = 'winrar.exe' && directory.dst contains '\\appdata\\local\\temp\\rar$'
- device.type = 'nwendpoint' && category = 'process event' && action = 'createprocess' && filename.src = 'winrar.exe' && param.dst contains '\\appdata\\local\\temp\\rar$' && filename.dst = 'cmd.exe','cscript.exe','powershell.exe','pwsh.exe','wscript.exe'

Guidance and Recommendations for Bumblebee (cont.)

YARA Rules:

- https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/BumbleBee.yar
- https://github.com/mikesxrs/Open-Source-YARA-rules/blob/master/Checkpoint/malware_bumblebee_packed.yar
- https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee

Historical IOCs:

- 0283fc3c0b8fc20696d7a93a41795e1f08e76fc45db57e377db57ee89079737d
- 655ffb98f0a773f6fb61bb7875ee4794efef3f619d785b1765d1fed7655d719e
- 7f573c17196a01fc9bdd0f8157e6b2508611a3f107123118e4c4ef2e05704026
- 8640824dd436af0e73c51a89aa86987f22fb76f60be94f61f3ae3affe5f0927e
- b8fe8d574d0e01d54eae49fbab316682a6ea810959af7db76a4d5a6a74d10280
- bb9fdc8b9c47ded76befa321ba947580ea8e1675e25b29e11dace720fbb9d6f6

Guidance and Recommendations for Bumblebee (cont.)

- c446284618132af527b171123c127cb389938f4b738d71022bb72b35553820ff
- 23.254.201.97:443
- 23.254.224.200:443
- 37.120.198.248:443
- 45.147.229.50:443
- 45.147.229.101:443
- 46.21.153.145:443
- 54.38.136.187:443
- 63.141.248.253:443
- 64.44.101.250:443
- 64.44.102.6:443
- 64.44.135.250:443
- 68.233.238.105:443
- 79.110.52.56:443
- 103.175.16.52:443
- 103.175.16.59:443
- 103.175.16.107:443
- 103.175.16.108:443
- 103.175.16.117:443
- 103.175.16.121:443
- 103.175.16.122:443
- 107.189.1.156:443
- 142.11.222.79:443
- 145.239.30.26:443
- 146.19.173.139:443
- 146.19.173.224:443
- 146.19.253.49:443
- 146.70.104.250:443
- 149.255.35.134:443
- 154.56.0.221:443
- 154.56.0.241:443
- 176.107.177.124:443
- 185.62.56.201:443
- 185.62.58.133:443
- 185.62.58.169:443
- 185.62.58.238:443
- 185.156.172.123:443
- 192.119.64.21:443
- 192.236.155.47:443
- 192.236.160.254:443
- 192.236.161.191:443
- 192.236.192.85:443
- 192.236.194.136:443
- 192.236.249.68:443
- 193.239.84.247:443
- 193.239.84.254:443
- 194.37.97.135:443
- 194.135.33.148:443
- 194.135.33.149:443
- 198.98.57.91:443
- 199.195.252.30:443
- 205.185.121.173:443
- 212.114.52.46:443
- newscommercde.com
- spkdeutshnewsupp.com
- germanysupportspk.com
- nrwmarkettoys.com

Guidance and Recommendations for Bumblebee (cont.)

MITRE ATT&CK Techniques:

- T1548.002 - Bypass User Account Control
- T1560 - Archive Collected Data
- T1059.001 - PowerShell
- T1059.003 - Windows Command Shell
- T1059.005 - Visual Basic
- T1132.001 - Standard Encoding
- T1005 - Data from Local System
- T1622 - Debugger Evasion
- T1140 - Deobfuscate/Decode Files or Information
- T1573.001 - Symmetric Cryptography
- T1041 - Exfiltration Over C2 Channel
- T1008 - Fallback Channels
- T1070.004 - File Deletion
- T1105 - Ingress Tool Transfer
- T1559.001 - Component Object Model
- T1036.005 - Match Legitimate Name or Location
- T1106 - Native API
- T1027 - Obfuscated Files or Information
- T1566.002 - Spearphishing Link
- T1057 - Process Discovery
- T1055 - Process Injection
- T1055.001 - Dynamic-link Library Injection
- T1055.004 - Asynchronous Procedure Call
- T1012 - Query Registry
- T1053.005 - Scheduled Task
- T1129 - Shared Modules
- T1518.001 - Security Software Discovery
- T1218.008 - Odbcconf
- T1218.011 - Rundll32
- T1082 - System Information Discovery
- T1033 - System Owner/User Discovery
- T1204.001 - Malicious Link
- T1204.002 - Malicious File
- T1497 - Virtualization/Sandbox Evasion
- T1497.001 - System Checks
- T1497.003 - Time Based Evasion
- T1102 - Web Service
- T1047 - Windows Management Instrumentation
- T1566.001 - Spearphishing Attachment

Guidance and Recommendations for IcedID

IcedID

IcedID is a banking trojan designed to steal financial information and credentials. It was first discovered in 2017 and has been downloaded by Emotet in multiple campaigns. IcedID is modular and can act as a loader for other viruses or modules.

NetWitness Logic:

- BazarLoader or IcedID URI Path

Hunting Queries:

- device.type = 'nwendpoint' && action = 'writetoexecutable','renametoexecutable' && filename.dst = 'passff.tar', 'cookie.tar'
- device.type = 'nwendpoint' && action = 'createprocess','openprocess' && filename.src = 'mshta.exe' && filename.dst = 'rundll32.exe','regsvr32.exe'
- ip.all = 206.188.197.218, 82.197.93.75 && service = 443, 80
- alias.host = 'b.citriix.org'

YARA Rules

- https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/IcedID.yar
- https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_IcedID.yar
- https://github.com/Neo23x0/signature-base/blob/master/yara/crime_icedid.yar

Historical IOCs:

- 8c637339dbf60797dd7b2c14812e6c5e275a28035d144f0398f2fe05b1e0d6db
- be6e2c4cee89968c5ef730b602cf9c9cdf6b3ab2a93cf62e6d39ed2048ac237151e8c7eaf3d
- c446284618132af527b171123c127cb389938f4b738d71022bb72b35553820ff

Guidance and Recommendations for IcedID (cont.)

- fe93144cb5400df8e2b9e311480b98e18573ae337e14b11a365b93385fca0cab
- 985e8bdc64b468222ff9f5c5156d170147d4596f62a069e066551997c0dee1e4
- 14cdead56b5ac59090b4a44c84deec61b66b467a8cbaa8880e9340b200f474a6
- d87c54a915466b0302f840cdcd0a76f6e27bd42809ceee6d8c0782de04f38bc1
- 39eb8393dba68b438f85bd139d824dd7c0afd95747533e3c3b77ad2eb4610232
- d09a83912636f5db10425cebaaccbd9401f25d62f0ab7baaef5a7dc02d409284
- 9d3c6abf1c366801e0948408952e23664bb761e9eef4e7173a40501d92750677
- 64785cd2fd7ccdd171a740f4b48852610ab8c683f1bef7672cb5f1de322a989a
- 70fca3fb7729be144051dba153278d09e02d27108d0c278f15ead28e7aa369ad
- 3db3341ac8691ada08f30cbde6f548559488015031dc21b6a97394bb3cb096b2
- 51620e007fc9cc703153ce086ecd6ddcbb61bb35e3d12fc8bf4faf88cc80c70b
- 96871674712afa004e06b7cff0f726349c1d4a238f1470044430858961eb7167
- 0a7963b659fbcc2ae2c56527c474071acf0e80a83a717baaa5a760480598d485
- 853b98974432f452e7e88005952b92ec655629abcafcc11555dfc7ca963ac5bf
- acci54.cyou
- bloadypupper.best
- boatergrip.top
- chessmate.top
- chinatrades.best
- 6c5e61019938feda5a94ed1075670544f379c8435017c950f8224
- d843d0016164e7ee6f56e65683985981fb14093ed79fde8e664b308a43ff4e79
- bb9fdc8b9c47ded76befa321ba947580ea8e1675e25b29e11dace720fbb9d6f6

Guidance and Recommendations for IcedID (cont.)

- customdrug.club
- felixheater.top
- fereware.club
- fillerwinner.best
- finderway.pw
- fleightfreight.best
- flightrewards.best
- forfillo.top
- fourgoun.co
- froplays.top
- gigafilliopot.pw
- gilogigamaster.best
- gilogigamaster.top
- hongcontrol.best
- ididallthis.best
- jeepwrangler.cyou
- kissavorob.best
- lookatamerica.best
- lovuterry.best
- luckyrobber.top
- mermateria.cyou
- morganholes.cyou
- newwheels.cyou
- northkorisla.co
- puppybloder.pw
- reavari.top
- rebuildcustom.pw
- shachess.cyou
- sweetyclass.top
- topolanger.best
- voltemeterz.top
- vosshodo.best
- warriordos.top
- warrioruno.top
- hxxps://scifimond[.]com/live/
- hxxps://drifajizo[.]fun/live/

Guidance and Recommendations for IcedID (cont.)

MITRE ATT&CK Techniques:

- T1027.002 - Software Packing
- T1027.003 - Steganography
- T1027.013 - Encrypted/Encoded File
- T1047 - Windows Management Instrumentation
- T1053.005 - Scheduled Task
- T1055.004 - Asynchronous Procedure Call
- T1059.001 - PowerShell
- T1059.003 - Windows Command Shell
- T1059.005 - Visual Basic
- T1069 - Permission Groups Discovery
- T1071.001 - Web Protocols
- T1082 - System Information Discovery
- T1087.002 Domain Account
- T1105 - Ingress Tool Transfer
- T1106 - Native API
- T1185 - Browser Session Hijacking
- T1204.002 - Malicious File
- T1218.007 - Msiexec
- T1547.001 - Registry Run Keys / Startup Folder
- T1566.001 - Spearphishing Attachment
- T1573.002 - Asymmetric Cryptography

Guidance and Recommendations for SystemBC

SystemBC

SystemBC is a Remote Access Trojan (RAT) written in Russian that was used as part of the attack chain in the DarkSide ransomware attack against the major American oil pipeline Colonial Pipeline. It has also been observed initializing Ransomware as a Service (RaaS) attacks such as Ryuk and Egregor. First seen in early 2019 but has evolved over time to carry out its C2s more discretely.

NetWitness Logic

- SystemBC will proxy network communication between an infected host and the attacker-controlled C2 server using SOCKS5. NetWitness Packets users can find SOCKS5 traffic by searching for "service = 1080". Any unexpected use or usage in conjunction with any of the previously listed NetWitness logic warrants further investigation.

YARA Rules:

- https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_SystemBC.yar
- https://malpedia.caad.fkie.fraunhofer.de/details/win.system

MITRE ATT&CK Techniques:

- T1010 - Application Window Discovery
- T1012 - Query Registry
- T1018 - Remote System Discovery
- T1027.002 - Software Packing
- T1059.001 - PowerShell
- T1071 - Application Layer Protocol
- T1082 - System Information Discovery
- T1083 - File and Directory Discovery

Guidance and Recommendations for SystemBC (cont.)

- T1033 - System Owner/User Discovery
- T1036 - Masquerading
- T1053 - Scheduled Task/Job
- T1055 - Process Injection
- T1056 - Input Capture
- T1057 - Process Discovery
- T1059 - Command and Scripting Interpreter
- T1087 - Account Discovery
- T1095 - Non-Application Layer Protocol
- T1105 - Ingress Tool Transfer
- T1106 - Native API
- T1124 - System Time Discovery
- T1497 - Virtualization/Sandbox Evasion
- T1518.001 - Security Software Discovery
- T1547 - Boot or Logon Autostart Execution
- T1547.001 - Registry Run Keys / Startup Folder
- T1560 - Archive Collected Data
- T1562.001 - Disable or Modify Tools
- T1564.001 - Hidden Files and Directories
- T1571 - Non-Standard Port
- T1573 - Encrypted Channel

Guidance and Recommendations for Pikabot

Pikabot

Pikabot, identified in May 2023, is a malicious software designed for cyber-attacks. It acts as a malware loader and backdoor, capable of executing commands and deploying payloads from a C2 server. This enables attackers to control an infected computer remotely. Notably, Pikabot is programmed to stop operating if it detects Russian or Ukrainian system languages, suggesting its operators may be from Russia or Ukraine.

The malware is notably spread through misleading ads and fake websites offering popular software like AnyDesk, Slack, and Zoom. Its growing popularity among cybercriminals stems from its ability to maintain stealthy, persistent remote access to victims' machines, facilitating the deployment of further malicious software. Pikabot also appeals to Ransomware-as-a-Service (RaaS) affiliates for its use of the TOR network, which helps hide their activities by encrypting and obscuring the malware's network traffic.

NetWitness Logic

- Pikabot uncommon extension execution by rundll detected

Hunting Queries:

- device.type = 'nwendpoint' && category = 'process event' && action = 'createprocess', 'openprocess', 'openosprocess' && filename.src = 'powershell.exe', 'cmd.exe', 'mshta.exe', 'cscript.exe', 'wscript.exe', 'msiexec.exe' && filename.dst = 'rundll32.exe'&& param.dst contains '\\appdata\\local\\temp', '\\programdata\\', '\\windows\\installer\\' && ~(param.dst contains '.dll')

Guidance and Recommendations for Pikabot (cont.)

- device.type = 'nwendpoint' && category = 'process event' && action = 'createprocess', 'openprocess', 'openosprocess' && filename.src = 'rundll32.exe' && filename.dst = 'seachprotocolhost.exe', 'searchfilterhost.exe'
- ((ip.all = 192.9.135.73 && port.all = 1194) || (ip.all = 172.234.250.178 && port.all = 2222))
- device.type = 'nwendpoint' && category = 'process event' && action = 'createprocess' && filename.src = 'searchprotocolhost.exe', 'searchfilterhost.exe' && ((param.src contains 'whoami','netstat','ipconfig') || (filename.dst ='whoami.exe', 'netstat.exe', 'ipconfig.exe'))

YARA:

- https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_PikaBot.yar
- https://github.com/kevoreilly/CAPEv2/blob/master/analyzer/windows/data/yara/Pikabot.yar
- https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/PikaBot.yar

Guidance and Recommendations for Pikabot (cont.)

Historical IOCs:

- 4ec643d9c0062fa2199b3999dc13ef9deb4b5fb9d890f3f03fdec9d5c9665e2c
- hxxps://109[.]199[.]99[.]131:13721
- hxxps://154[.]38[.]175[.]241:13721
- hxxps://148[.]113[.]141[.]220:2224
- hxxps://23[.]226[.]138[.]143:2083
- hxxps://89[.]117[.]23[.]186:5686
- hxxps://23[.]226[.]138[.]161:5242
- hxxps://103[.]82[.]243[.]5:13721
- hxxps://145[.]239[.]135[.]24:5243
- hxxps://185[.]179[.]217[.]216:9785
- hxxps://154[.]12[.]248[.]41:5000
- hxxps://178[.]18[.]246[.]136:2078
- hxxps://141[.]95[.]106[.]106:2967
- hxxps://104[.]129[.]55[.]105:2223
- hxxps://57[.]128[.]165[.]176:13721
- hxxps://89[.]117[.]23[.]185:2221
- hxxps://86[.]38[.]225[.]106:2221
- hxxps://37[.]60[.]242[.]86:2967
- hxxps://37[.]60[.]242[.]85:9785
- hxxps://89[.]117[.]23[.]34:5938
- hxxps://154[.]12[.]233[.]66:2224

Guidance and Recommendations for Pikabot (cont.)

MITRE ATT&CK Techniques:

- T1016 – System Network Configuration Discovery
- T1027.007 – Dynamic API Resolution
- T1033 – System Owner/User Discovery
- T1041 – Exfiltration Over C2 Channel
- T1053 – Scheduled Task
- T1055.002 – Portable Executable Injection
- T1055.003 – Process Hollowing
- T1055.003 – Thread Execution Hijacking
- T1057 – Process Discovery
- T1059.003 – Windows Command Shell
- T1071.001 – Web Protocols
- T1083 – File and Directory Discovery
- T1087.001 – Local Account
- T1087.002 – Domain Account
- T1106 – Native API
- T1129 – Shared Modules
- T1140 – Deobfuscate/Decode Files or Information
- T1482 – Domain Trust Discovery
- T1497.001 – System Checks
- T1497.003 – Time Based Evasion
- T1547.001 – Registry Run Keys / Startup Folder
- T1571 – Non-Standard Port
- T1573.001 – Symmetric Cryptography
- T1614.001 – System Language Discovery
- T1622 – Debugger evasion

Guidance and Recommendations for Smoke Loader

Smoke Loader

Smoke Loader is a significant botnet known for delivering a large volume of payloads, often by loading other stages of malware. Since its identification in 2011, Smoke Loader has become a prominent tool in the malware distribution scene, supported by its widespread availability and association with numerous bot networks.

Operation Endgame's takedown was a pivotal operation against Smoke Loader, resulting in the seizure and inaccessibility of multiple associated bot networks. Despite the success of these efforts, not all networks distributing Smoke Loader were seized. Only a single operator, superstar75737, representing a handful of bot networks, has the current botnet infrastructure taken down. SuperStar75737 has been active since at least 2022.

Less than a year ago, some of the superstar75737 personas used to register domains, and some of its infrastructure, including hash-busting URLs and randomized malware samples, continued to deliver ransomware until Operation Endgame.

Hunting Queries:

- filename.src contains 'toolspab', 'game'
- ip.all = 185.215.113.68, 95.217.43.206
- alias.host contains 'coin-coin-coin', 'data-host-file', 'host-coin-data', 'privacy-tools-for-you', 'rixoxeu9', 'planilhasvbap', 'telegatt'

YARA:

- https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_Smokeloader.yar
- https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader

Guidance and Recommendations for Smoke Loader (cont.)

Historical IOCs:

- https://coin-coin-coin-2[.]com/downloads/toolspab2.exe
- https://coin-coin-coin-2[.]com/downloads/toolspab4.exe
- https://data-host-file-16[.]com/downloads/toolspab2.exe
- https://host-coin-data-1[.]com/downloads/toolspab1.exe
- https://privacy-tools-for-you-453[.]com/downloads/toolspab4.exe
- https://privacy-tools-for-you-780[.]com/downloads/toolspab3.exe
- 168d41799cdb359a86c7e28e4b3eee3494270ec6e2884452dd61134b627b1c68
- 8a56cecfe36b7c105401fd246f8f3ba97bdc4d1db776eaa4991fcedf8aaaaa52
- ff6d6f616687fac25a1d77e52024838239e9a3bbb7b79559b0439a968ac384fe
- Ba8533bd8118ec6881e25e4af2e2101996b4a9aef3f1f1931423bff03da0ace5
- 4e1f743b60d65732d43e6a8c064016369a2cb6d03e81e04e114ed6a31297a2a7

Guidance and Recommendations for Smoke Loader (cont.)

MITRE ATT&CK Techniques:

- T1027.013 - Encrypted/Encoded File
- T1053.005 - Scheduled Task
- T1055 - Process Injection
- T1055.012 - Process Hollowing
- T1059.005 - Visual Basic
- T1071.001 - Web Protocols
- T1083 - File and Directory Discovery
- T1114.001 - Local Email Collection
- T1497.001 - System Checks
- T1547.001 - Registry Run Keys / Startup Folder

T1552.001 - Credentials In Files

- T1555.003 - Credentials from Web Browsers
- T1140 -Deobfuscate/Decode Files or Information

Guidance and Recommendations for TrickBot

TrickBot

TrickBot, aka TrickLoader, which has merged with now-defunct Conti, is a banking Trojan that targets both businesses and consumers. Trickbot, first identified in 2016 and continuously updated, poses a significant threat by targeting sensitive data such as banking details, account credentials, personally identifiable information (PII), and bitcoins. With its ability to laterally move within networks through exploits, disseminate through Server Message Block (SMB) shares, deploy additional malware like Ryuk ransomware, and search for valuable files on compromised hosts, Trickbot showcases a high level of sophistication. It also employs a unique crypter to repackage existing malware, circumventing standard network defenses. Additionally, Trickbot offers its custom crypter to affiliated crimeware gangs, including Emotet, and it is rumored to be available to various Ransomware-as-a-Service (RaaS) groups, such as Maze. Its crypting service is notably versatile, supporting an array of crypters like TrickCrypt (aka VirtualAllocExNumA), AC27, Dave, and others, furthering its utility and threat level within cybercriminal ecosystems.

MITRE ATT&CK Techniques:

- T1027.009 - Encrypted/Encoded File
- T1027.013 - Embedded Payloads