ScrubCrypt Deploys VenomRAT with an Arsenal of Plugins

Date: 10th April 2024 | Severity: High

Summary

ScrubCrypt has been described as an “antivirus evasion tool” that converts executables into undetectable batch files. It offers several options to manipulate malware, making it more challenging for antivirus products to detect.

It was recently discovered a threat actor distributing a phishing email containing malicious Scalable Vector Graphics (SVG) files. The email lures victims into clicking on an attachment, which downloads a ZIP file containing a Batch file obfuscated with the BatCloak tool. ScrubCrypt is then used to load the final payload, VenomRAT while maintaining a connection with a command and control (C2) server to install plugins on victims’ environments. The plugin files downloaded from the C2 server include VenomRAT version 6, Remcos, XWorm, NanoCore, and a stealer designed for specific crypto wallets.

Attack Vectors

- The attacker initiates the attack by sending a phishing email stating that a shipment has been delivered. It also includes an attached invoice. The attachment is an SVG file named “INV0ICE_#TBSBVS0Y3BDSMMX.svg,” which contains embedded base64-encoded data.This HTML file directs users to a malicious link. The attackers employ evasion techniques such as using temporary domains and country-specific redirects.
- After victims open the SVG file, the ECMAScript creates a new blob and utilizes “window.URL.createObjectURL” to drop the decoded data as a ZIP file named “INV0ICE_#TBSBVS0Y3BDSMMX.zip.”
- The script initially copies a PowerShell execution file to “C:\Users\Public\xkn.exe” and utilizes the copied file in later commands. It includes parameters in each command, “-WindowStyle hidden -inputformat none -outputformat none -NonInteractive,” to conceal its activity from the victim’s notice. It then decodes the malicious data and saves it as “pointer.png.” After hex-decoding, the result is saved as a “pointer” and moved to “C:\Users\Public\Libraries\pointer.cmd.” Upon executing “pointer.cmd,” it employs “cmd /c del” to delete all the files mentioned above.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 0f1d6aab547ceca6e71ac2e5a54afdaea597318fe7b6ca337f5b92fdff596168 • 06779e1015bd7dd2012ad03f7bb3f34e8d99d6ca41106f89cb9fb1ec46fe034e • 0b5631041336a58ab859d273d76c571dd372220dfa1583b597a2fe5339ad4bf7 • 2373840bc455d601551304ec46c281b218e90a91dce3823709c213814636e899 • 258578c03ca314ac3a636a91e8b3245230eae974cf50799d89b3f931e637014c • 411ad772af94a042413af482a2ef356d3217bcc5123353e3c574347cb93e3d5a • 4a4b5c22c877437c359ef2acaeeb059881da43b11798581cf2f31c2c83fc3418 • 4cda23993d793ef070be7b9066f31a45b10c1e72d809f4a43726da977a0069d8 • 51ecf11a64e934409bfada2b6f0c4d89c3420ca95640bc88f928906e6f0b4832 • 53a522051e0319176dece493b7e2543135ed41c402adbfeda32a5f6be7d68175 • 546a85e384ced3d4535bad16a877ecd36a79849c379c5daa357689116f042c1b • 5c5caa3182d6b121c1445d6ca81134ec262cd5ea4f9ef1944f993b63d1987647 • 5f1746b4bd8d94d4d3feb1e2d4a829b6c3bab9341e272341f4b3a1da01d20745 • 6aaff578555cb82159a9c16a159f0437c39b673744e0c537c4b7f0f67f56c5d9 • 6ac5c7284aaa0c195723df7a78ae610a7ee096b3b5bc19f6838451acd438116e • 71a22bed7ab5a26158fc1cf1b7bb87146254672483aad72736817ff16e656c7b • 7d7a710e3c0e5da830213f9b72f44a72d721adcf17abc838f28286dde8a1e8d9 • 7d9c8d44554ee10310805920afb51249a1e8cd3e32b430e8c9638fec316913d3 • 85790dad1a0af5febd7d90e0ec9ce680ec87dcc31a94a25bfb454bb121164bfd • 8e97019f8c4712f1fc9728c4706112a5ef85a05aa809985709faef951925e094 • 94b2e06e45407f193cfe58e18f5c250bbd1b8e857a754f1c366913129b9dada7 • bee35a9d30d6f69cd6d173c6a6a93110cac59ab3710e32eced6f266581e88b87 • cd1364d8c7f6f0246ed91cd294e2e506e7c94ba2f9a33c373c6fcfe04bbe17e7 • d04bf1a9f6014bf4bcdb3ac4eb6d85bcc4159ae25a7f00c4493cbcb8e892e159 • d05ad3dc62e1dc45fd31dc2382c1ea5e5f26f4f7692cb2ef8fd1c6e74b69fa16 • dc2c1694d363d78cdfed0574cf51413b9b48d932e076033bb76cf69a4470b7e9 • dceea68a037376b323d2a934f9fdc59bfbd2c2c0ed66014bdf059f403f4dc6f2 • e190d172b7d3c7f1055052f0ed3da5d5979a8a2b622ca2fbcea90774a5bf6008 • f02c04bc428694a11917375f41ecb7c7aa326cf242b4c56ed1e7b3ae14d5dd68 • f4164be3d357682754559aa32ea74c284eee64140d3f56a63a225d5de10d051c
Domains	• hjkdnd[.]duckdns[.]org • rachesxwdavid[.]duckdns[.]org • mup830634[.]duckdns[.]org • markjohnhvncpure[.]duckdns[.]org • homoney177[.]duckdns[.]org • febvenom8[.]duckdns[.]org
URLs	• hxxps://nanoshd[.]pro/files/new_image.jpg?14441723 • hxxps://nanoshield[.]pro/new_image2.jpg?166154725 • hxxps://kisanbethak[.]com/P/ • hxxps://kisanbethak[.]com/K/

Recommendation

- Email Filtering
- Endpoint Protection
- Patch Management
- Incident Response Plan
- Vendor Risk Management
- Regular Security Audits

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.fortinet.com/blog/threat-research/scrubcrypt-deploys-venomrat-with-arsenal-of-plugins