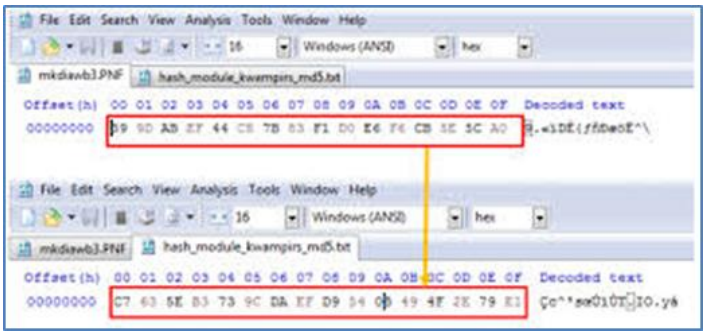
TACTICAL CYBER INTELLIGENCE

SERIAL: WR-20-038-001
REPORT DATE: 02072020
COUNTRY: US

Kwampirs Malware IoC's Attacking Supply Chain in Global Industries

Summary:

The US FBI is providing indicators of compromise (IoC) for the two identified modules of the Kwampirs Remote Access Trojan (RAT). The FBI has identified additional information regarding the Kwampirs RAT, which has targeted several global industries, including the software supply chain, healthcare, energy, and financial sectors. Software supply chain companies are believed to be targeted in order to gain access to the victim's strategic partners and/or customers, including entities supporting Industrial Control Systems (ICS) for global energy generation, transmission, and distribution. The Kwampirs RAT has been observed by the FBI supporting targeted computer intrusions on these sectors, including supporting additional module execution on the targeted victim network, believed to enable follow-on computer network exploitation operations.[1]



While the Kwampirs RAT has not been observed incorporating a wiper component, comparative forensic analysis has revealed the Kwampirs RAT as having numerous similarities with the data destruction malware Disttrack (commonly known as Shamoon). To assist with identification of the Kwampirs RAT, the FBI is providing five YARA rules, which produce consistent results on open source tools, such as Virus Total and Hybrid Analysis, for the Kwampirs RAT and Shamoon malware.

Technical Details:

Rule Kwampirs_Shamoon_Code
{ meta: yara_version = "3.7.0" date = "14 Jan 20" description = "Kwampirs and Shamoon common code" strings: $memcpy = { 56 8B F0 85 FF 74 19 85 D2 74 15 8B CF 85 F6 74 0B 2B D7 8A 04 0A 88 01 41 4E 75 F7 8B C7 5E C3 33 C0 5E C3 } $strlenW = { 33 C0 85 C9 74 17 80 3C 41 00 75 07 80 7C 41 01 00 74 0A 3D 00 94 35 77 73 03 40 EB E9 C3 } $strcmp = { 85 C0 75 07 85 D2 75 40 B0 01 C3 85 D2 74 39 66 83 38 00 56 74 24 0F B7 0A 66 85 C9 74 16 66 8B 30 83 C2 02 83 C0 02 66

[1] FBI Flash Report CP-000118-MW, dtd 5 FEB 2020

3B F1 75 18 66 83 38 00 75 E4 EB 06 66 83 38 00 75 0A 66 83 3A 00 75 04 B0 01 5E C3 32 C0 5E C3 32 C0 C3 } condition: uint16(0) == 0x5a4d and 1 of them }

Rule Kwampirs_Installer
{ meta: yara_version = "3.7.0" date = "14 Jan 20" description = "Kwampirs installer xor keys and Unicode string length routine" strings: $string_key = { 6C 35 E3 31 1B 23 F9 C9 65 EB F3 07 93 33 F2 A3 } $resource_key = { 28 99 B6 17 63 33 EE 22 97 97 55 B5 7A C4 E1 A4 } $strlenW = { 33 C0 85 C9 74 17 80 3C 41 00 75 07 80 7C 41 01 00 74 0A 3D 00 94 35 77 73 03 40 EB E9 C3 } condition: uint16(0) == 0x5a4d and 2 of them }

Rule Kwampirs_Implant { meta: yara_version = "3.7.0" date = "14 Jan 20" description = "Kwampirs implant xor and rsa keys" strings: $string_key = { 6C 35 E3 31 1B 23 F9 C9 65 EB F3 07 93 33 F2 A3 } $beacon_key = { 28 30 A4 3F 6D 28 04 23 36 2A 32 DC AD 0B A0 4B E8 20 1F 64 84 0A F4 C4 C7 8A 8D C0 A2 C4 40 19 A1 43 82 38 14 FD 6C 90 E0 7E 2A 40 DF D3 F2 3E 72 38 C4 96 4D 98 7C 16 3B 3C E7 27 B7 D0 EF 7B 3C 45 06 9A 69 0D 6A 41 18 95 95 46 88 CC 19 6F EB 6B 5B F8 51 E4 2E E1 E6 8F 44 CF 20 2F 2B DE 7A 28 5D DB 55 5A 1A 35 AF D8 5F 57 B8 0F A5 F7 08 4A D0 AB E5 95 31 A1 25 31 00 65 3C 70 73 99 42 0A 02 1A 69 D9 A6 DF 14 B2 05 DD A8 DF F5 D9 71 6D 6E 96 5F 1B D1 0F 8E 0A 35 D4 65 FA 90 58 CC 75 02 92 B7 2C 46 ED 66 33 44 75 FC A4 E0 FD B8 C8 B5 0C 3A 84 D9 23 16 A4 AF 3B 57 C6 D2 5C B3 AB 9C CD F0 B2 A4 51 43 D3 F0 30 21 B5 ED 25 E3 64 B7 0C 1C A8 50 3A FF 6B 2C 32 06 B2 D1 54 3D 86 B9 1A BF 59 D7 92 59 EC 40 4A 8D B0 E7 9A 9A 0D 94 19 27 D8 6D AD 5C 3E BE 14 67 DC F0 92 } $download_key = { B7 E9 F9 2D F8 3E 18 57 B9 18 2B 1F 5F D9 A5 38 C8 E7 67 E9 C6 62 9C 50 4E 8D 00 A6 59 F8 72 E0 91 42 FF 18 A6 D1 81 F2 2B C8 29 EB B9 87 6F 58 C2 C9 8E 75 3F 71 ED 07 D0 AC CE 28 A1 E7 B5 68 CD CF F1 D8 2B 26 5C 31 1E BC 52 7C 23 6C 3E 6B 8A 24 61 0A 17 6C E2 BB 1D 11 3B 79 E0 29 75 02 D9 25 31 5F 95 E7 28 28 26 2B 31 EC 4D B3 49 D9 62 F0 3E D4 89 E4 CC F8 02 41 CC 25 15 6E 63 1B 10 3B 60 32 1C 0D 5B FA 52 DA 39 DF D1 42 1E 3E BD BC 17 A5 96 D9 43 73 3C 09 7F D2 C6 D4 29 83 3E 44 44 6C 97 85 9E 7B F0 EE 32 C3 11 41 A3 6B A9 27 F4 A3 FB 2B 27 2B B6 A6 AF 6B 39 63 2D 91 75 AE 83 2E 1E F8 5F B5 65 ED B3 40 EA 2A 36 2C A6 CF 8E 4A 4A 3E 10 6C 9D 28 49 66 35 83 30 E7 45 0E 05 ED 69 8D CF C5 40 50 B1 AA 13 74 33 0F DF 41 82 3B 1A 79 DC 3B 9D C3 BD EA B1 3E 04 33 } $hashfile_key = { FE FE F5 5C 37 54 A1 6C 28 84 ED BF 84 70 25 41 56 24 37 32 98 9F A0 35 48 F3 1C 33 2E F9 D0 A3 7D 36 BA 66 ED FB 52 E3 8B 07 32 5A 1A DD 19 0A F0 73 A8 C6 61 3F 3F 31 8A 93 AB F4 19 AA D8 42 3B 3E 6E FC 0A 2A 41 1B 28 33 7F 79 27 41 81 14 D0 0B 24 06 4C 35 B3 23 5C F2 E4 06 7D 73 93 1C 7A 30 8E 87 74 0F 53 F9 92 A3 CA 20 E3 A1 12 E1 6B 86 62 B6 CC C1 45 C9 43 43 15 59 BE 5A 77 31 D8 36 5F BD F6 D7 09 65 42 3C CD 2C B1 C1 28 55 6E F9 91 3C 55 3B DF EB ED BF 84 70 25 41 56 24 37 32 98 9F A0 35 48 F3 1C 33 2E F9 D0 A3 7D 36 BA 66 ED FB 52 E3 8B 07 32 5A 1A DD 19 0A F0 73 A8 C6 61 3F 3F 31 8A 93 AB F4 19 AA D8 42 3B 3E 6E FC 0A 2A 41 1B 28 33 7F 79 27 41 81 14 D0 0B 24 06 4C 35 B3 23 5C F2 E4 06 7D 73 93 1C 7A 30 8E 87 74 0F 53 F9 92 A3 CA 20 E3 A1 12 E1 6B 86 } $rsa_key = { CD 74 15 BC 47 7E 0A 5E E4 35 22 A5 97 0C 65 BE E0 33 22 F2 94 9D F5 40 97 3C 53 F9 E4 7E DD 67 CF 5F 0A 5E F4 AD C9 CF 27 D3 E6 31 48 B8 00 32 1D BE 87 10 89 DA 8B 2F 21 B4 5D 0A CD 43 D7 B4 75 C9 19 FE CC 88 4A 7B E9 1D 8C 11 56 A6 A7 21 D8 C6 82 94 C1 66 11 08 E6 99 2C 33 02 E2 3A 50 EA 58 D2 A7 36 EE 5A D6 8F 5D 5D D2 9E 04 24 4A CE 4C B6 91 C0 7A C9 5C E7 5F 51 28 4C 72 E1 60 AB 76 73 30 66 18 BE EC F3 99 5E 4B 4F 59 F5 56 AD 65 75 2B 8F 14 0C 0D 27 97 12 71 6B 49 08 84 61 1D 03 BA A5 42 92 F9 13 33 57 D9 59 B3 E4 05 F9 12 23 08 B3 50 9A DA 6E 79 02 36 EE CE 6D F3 7F 8B C9 BE 6A 7E BE 8F 85 B8 AA 82 C6 1E 14 C6 1A 28 29 59 C2 22 71 44 52 05 E5 E6 FE 58 80 6E D4 95 2D 57 CB 99 34 61 E9 E9 B3 3D 90 DC 6C 26 5D 70 B4 78 F9 5E C9 7D 59 10 61 DF F7 E4 0C B3 } condition: uint16(0) == 0x5a4d and 2 of them }

Rule KwampirsBase64 { meta: date = "14 Jan 20" description = "Kwampirs Base64 encoding decoding routine closely based on open source C plus plus functions"

strings:

$b64_long_match = { 8A DA 8A C1 C0 EB 04 80 E1 03 C0 E1 04 02 CB [4] 80 E2 0F 02 D2 C0 EB 06 02 D2 02 D3 [3] (80 E3 3F C0 E8 02 | C0 E8 02 80 E3 3F) 83 3D }

condition: (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and $b64_long_match }

Rule Kwampirs_Shamoon { meta: date = "14 Jan 20" description = "Kwampirs Shamoon overlap" strings: $s1 = "g\\system32\\" fullword wide $s2 = "ztvttw" fullword wide $s3 = "lwizvm" fullword ascii

$op1 = { 94 35 77 73 03 40 eb e9 } $op2 = { 80 7c 41 01 00 74 0a 3d } $op3 = { 74 0a 3d 00 94 35 77 } condition: (uint16(0) == 0x5a4d and filesize < 4000KB and 3 of them) }

Recommended Actions Post-Infection:

If a Kwampirs RAT infection is detected, contact your IT mitigation and remediation company and coordinate your mitigation efforts with your local FBI field office. The following information would assist the FBI's investigation of this malware:

- Full capture of network traffic in PCAP format from the infected host(s) (48 hour capture).
- Full image and memory capture of infected host(s).
- Web proxy logs capture, to include cache of the Web proxy.
- DNS and firewall logs.
- Identification and description of host(s) communicating with the C2 (ex: server, workstation, other).
- Identification of patient zero and attack vector(s), if able.

Best Practices for Network Security and Defense:

- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Establish, and backup offline, a "known good" version of the relevant server and a regular changemanagement policy to enable monitoring for alterations to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities.
- Implement a least-privileges policy on the Web server to: o Reduce adversaries' ability to escalate privileges or pivot laterally to other hosts. o Control creation and execution of files in particular directories.
- If not already present, consider deploying a demilitarized zone (DMZ) between the Web-facing systems and corporate network. Limiting the interaction and

logging traffic between the two provides a method to identify possible malicious activity.
- Ensure a secure configuration of Web servers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.
- Use a reverse proxy or alternative service to restrict accessible URL paths to known legitimate ones.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero-day attacks, it will highlight possible areas of concern.
- Deploy a Web application firewall and conduct regular virus signature checks, application fuzzing, code reviews, and server network analysis.

Conclusion:

Red Sky Alliance strongly recommends heeding the above recommendations and conduct ongoing monitoring from both internal and external perspectives. Internal monitoring is common practice. However, external threats are often overlooked and can represent an early warning of impending attacks. Red Sky Alliance can provide both internal monitoring in tandem with RedXray notifications on external threats to include, botnet activity, public data breaches, phishing, fraud, and general targeting. Red Sky Alliance is located in New Boston, NH USA. We are a Cyber Threat Analysis and Intelligence Service organization. For questions, comments or assistance, please contact the lab directly at 1-844-492-7225, or feedback@wapacklabs.com

Interested in a RedXray subscription to see what we can do for you? Sign up here: https://www.wapacklabs.com/redxray

Reporting: https://www.redskyalliance.org/
Website: https://www.wapacklabs.com/
LinkedIn: https://www.linkedin.com/company/wapacklabs/
Twitter: https://twitter.com/wapacklabs?lang=en