Akira Ransomware

Date: 23rd April 2024 | Severity: High

Summary

The Akira ransomware group, first reported by cybersecurity researchers in May 2023, has been active since at least March 2023 (it does not appear to be related to the 2017 ransomware operation of the same name). The group primarily targets North American organizations from various sectors, such as education, finance, real estate, manufacturing, and consulting.

Attack Vectors

- Akira installs a Cloudflare tunnel (cloudflared.exe) to establish remote access to the victim's network. In addition, the threat actors use the Netscan tool to perform network reconnaissance and leverage Mimikatz and the DonPAPI credential theft toolkit to dump credentials (such as RDP credentials, browser cookies, and VNC passwords) for further infiltration. Using the acquired credentials, the attackers move laterally in the victim's network (primarily using RDP). They also create an account on a compromised domain controller using a common naming convention to blend in the system.
- Before the encryption, Akira exfiltrates valuable data (for example, business-related documents), disables Microsoft Defender, shuts down the Windows Restart Manager API and other processes that might interfere with the encryption process, and uses a PowerShell command to delete volume shadow copies preventing easy system recovery. Then, the ransomware encrypts files (using the RSA and AES encryption algorithms) while appending them with the .akira extension. Notably, since August 2023, Akira has began deploying a Rust-based ransomware variant, Megazord, that encrypts files while appending them with the .powerrangers extension. To prevent rendering the system unusable, Akira does not encrypt certain Windows system files and files that are found in the Recycle Bin, System Volume Information, Boot, ProgramData, and Windows folders. At the end of the encryption process, a ransom note (akira_readme.txt) is dropped in every folder. The group's ransom demands range from $200,000 to millions of dollars.
- Akira operates an active leak site (designed with retro green colors), in which it uploads the data of victims who refused to pay the ransom. The leak site also enables victims to chat with the threat actors using a unique negotiation password.Commonly used tools: AdFind, Advanced IP Scanner, AnyDesk, LaZagne, PCHunter64, Mimikatz, Ngrok, RClone, SoftPerfect, and WinSCP.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• dynsys.is-a-guru[.]com • websites.theworkpc[.]com • rec.casacam[.]net • akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion • srxy123.is-a-geek[.]com • s1-filecr[.]xyz • 51-83-136-132[.]xyz • samaerx.ddnsfree[.]com • foxn1.sells-it[.]net • fon1.sells-it[.]net
File Hash	• eb6dc793918d46556ea79531e49d5e12bb237802218abd8cdaa115752431b07a • c3e3b2159fc97bdc7904c539c6195a47baadd36d73e511c31980f6a08073d9a4 • c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0 • 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a • 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50 • 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0 • 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4 • 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88 • 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d • 74fc20b6715fa1318455dca3a979afeb340c8fe03cdfa43dce8469fa36f7f78c • 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4 • 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c • 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf • 1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e • 1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc • 1ed8c04e2e91c9db7b88f818cc7d8f043f674d1898c182b6390acaa9fbb251aa • 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07 • d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959 • 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32 • e74f3881764f0469ac6d67379fbcc837ddbc753d019a0ba35ce97abe550453ad • ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc • 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c • f151257e38fc27b81eb3bdf694175d0872c9e0438fc5ea08844c912487290e75 • 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be • 92072945358b605c024b9e3335fb33b82faf33048c56f5529aaf5af4bf0c1b30 • d371ee0aa4fa710c00173d296c999a5497a18b38c80095db68a2dc5e46ed35f7 • 8738ba49fcd520789569aea7bf7af890741a745c79ae2bef49b93fb46c076c2b • c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777 • 82e25f32e01f1898ccce2b6d5292245759733c22a104443a8a9c7db1ebf05c57 • fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776
IP	• 1Domain27[.]60[.]236 • 148[.]72[.]168[.]13 • 148[.]72[.]171[.]171 • 138[.]124[.]184[.]174 • 91[.]132[.]92[.]60 • 141[.]95[.]84[.]40 • 176[.]124[.]201[.]200 • 27[.]1[.]0[.]189 • 16[.]1[.]0[.]106 • 13[.]70[.]2[.]40 • 14[.]1[.]9[.]124 • 1[.]94[.]147[.]103 • 108[.]143[.]240[.]80 • 185[.]205[.]209[.]206
URL	https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments..

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.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
- https://www.cyberdaily.au/security/10465-akira-ransomware-made-us-42m-in-ransoms-before-its-first-birthday