NYOTRON ATTACK RESPONSE CENTER

SamSam Ransomware Report

April 2018

NYOTRON
SECURING THE WORLD

Intel Report

During March 2018, a ransomware outbreak struck several US organizations, including the City of Atlanta and the City of Baltimore (its 911 emergency system). These attacks caused serious damage and disrupted work activity within the attacked organizations.

Although the latest wave of attacks appears to be the most significant one, the first wave of the SamSam ransomware was spotted as early as late 2017.

Attack Vector

While it is still unclear how attackers penetrate internal networks, most reports suggest that web-facing services such as SMB, RDP, VNC and JBoss are likely the initial access vector to the network.

By analyzing past reports of the responsible group's modus operandi, attackers first penetrate the network and then try to expand their control. This is usually done using known tools such as Mimikatz, PowerShell and more. Once attackers have enough control over the network and have managed to disable an organization's backup plan, they run the ransomware on a targeted host in a semi-automatic fashion.

SamSam Ransomware

Authors of the current widespread SamSam variant have invested significant effort in anti-forensic techniques. To this end, they split the malware into two components: a loader and an encrypted binary. Upon running, the loader decrypts the encrypted binary in memory using a provided key, and deletes the encrypted binary from the disk once decrypted. The now-decrypted code is responsible for the damage done by the malware, such as encryption of user files and ransom-note display. After completion of the malicious payload, the malware deletes itself from the drive.

Indicators of Compromise

SHA256 (of loaders)

- 0785bb93fdb219ea8cb1673de1166bea839da8ba6d7312284d2a08bd41e38cb9
- 338fdf3626aa4a48a5972f291aacf3d6172dd920fe16ac4da4dd6c5b999d2f13
- 3531bb1077c64840b9c95c45d382448abffa4f386ad88e125c96a38166832252
- 4856f898cd27fd2fed1ea33b4d463a6ae89a9ccee49b134ea8b5492cb447fb75
- 516fb821ee6c19cf2873e637c21be7603e7a39720c7d6d71a8c19d8d717a2495
- 72832db9b951663b8f322778440b8720ea95cde0349a1d26477edd95b3915479
- 754fab056e0319408227ad07670b77dde2414597ff5e154856ecae5e14415e1a
- 88d24b497cfeb47ec6719752f2af00c802c38e7d4b5d526311d552c6d5f4ad34
- 88e344977bf6451e15fe202d65471a5f75d22370050fe6ba4dfa2c2d0fae7828
- 8eabfa74d88e439cfca9ccabd0ee34422892d8e58331a63bea94a7c4140cf7ab
- 8f803b66f6c6bc4da9211a2c4c4c5b46a113201ecaf056d35cad325ec4054656
- dabc0f171b55f4aff88f32871374bf09da83668e1db2d2c18b0cd58ed04f0707
- e7bebd1b1419f42293732c70095f35c8310fa3afee55f1df68d4fe6bbee5397e

Bitcoin Wallet

- 1HbJu2kL4xDNK1L9YUDkJnqh3yiC119YM2

Tor Onion Service

- jcmi5n4c3mvgtyt5.onion/nonpenetrable/

PARANOID

While the Nyotron Research Team is still investigating the full scope of the latest events, they have analyzed previous versions of the attack, resulting in successful prevention by PARANOID. In conjunction with Cisco Talos' statement that the encryption mechanism has not changed (see full report here), the Nyotron Research Team has strong evidence suggesting that PARANOID would also prevent the latest variant of the attack.

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com