Rewterz Threat Alert - New Ransomware Actor OldGremlin Hits Multiple Organizations - Rewterz

Published: 2020-09-24 · Archived: 2026-04-05 16:40:40 UTC

Severity

High

Analysis Summary

A new ransomware group has been targeting large corporate networks using self-made backdoors and file-encrypting malware for the initial and final stages of the attack. Codename OldGremlin is used for the group. Security experts suspect that OldGremlin is currently operating at smaller scale to fine-tune their tools and techniques before going global. OldGremlin is using custom backdoors (TinyPosh and TinyNode) and ransomware (TinyCrypt, a.k.a decr1pt) along with third-party software for reconnaissance and lateral movement (Cobalt Strike, command line screenshot, NirSoft's Mail PassView for email password recovery). The group has so far targeted medical labs, banks, manufacturers, software developers, etc.

The threat actor starts its attacks with spear phishing emails that deliver custom tools for initial access. They use valid names for the sender address, impersonating well-known individuals. The emails contain links that download the TinyPosh backdoor. The aim is to gain a foothold on the target organization's network via one of the two backdoors (TinyNode or TinyPosh) that allow expanding the attack via additional modules downloaded from their command and control (C2) server. Remote Desktop Protocol is also used to jump to other systems on the network. After spending some time on the network identifying valuable systems, the attacker deploys the file-encrypting routine. In the case of a medical laboratory, the attacker obtained domain administrator credentials and created a fallback account with the same elevated privileges to maintain persistence in case the initial one was blocked. OldGremlin moved to the encryption stage a few weeks after the initial access, deleting server backups and locking hundreds of computers on the corporate network. The ransom note left behind asked close to $50,000 in cryptocurrency for the decryption key and provided a Proton email address for contact.

Impact

- Credential Theft
- Unauthorized Access
- Files Encryption
- Information Theft
- Network-wide Infection

Indicators of Compromise

Domain Name

- ksdkpwpfrtyvbxdobr1[.]tiyvbxdobr1[.]workers[.]dev
- wispy-fire-1da3[.]nscimupf[.]workers[.]dev
- noisy-cell-7d07[.]poecdjusb[.]workers[.]dev
- hello[.]tyvbxdobr0[.]workers[.]dev
- wispy-surf-fabd[.]bhrcaoqf[.]workers[.]dev
- broken-poetry-de86[.]nscimupf[.]workers[.]dev
- calm-night-6067[.]bhrcaoqf[.]workers[.]dev
- rough-grass-45e9[.]poecdjusb[.]workers[.]dev
- ksdkpwprtyvbxdobr0[.]tyvbxdobr0[.]workers[.]dev
- curly-sound-d93e[.]ygrhxogxiogc[.]workers[.]dev
- old-mud-23cb[.]tkbizulvc[.]workers[.]dev
- rbcholding[.]press

MD5

- f30e4d741018ef81da580ed971048707
- 94293275fcc53ad5aca5392f3a5ff87b
- 2c6a9a38ace198ab62e50ab69920bf42
- fc30e902d1098b7efd85bd2651b2293f
- e0fe009b0b1ae72ba7a5d2127285d086
- 306978669ead832f1355468574df1680
- e1692cc732f52450879a86cb7dcfbccd
- e47a296bac49284371ac396a053a8488
- 30fdbf2335a9565186689c12090ea2cf

SHA-256

- 71f351c47a4cd1d9836b39da8454d1dc20df51950fe1c25aa3192f0d60a0643f
- d3082e2737ab637ee7ee09473ad51c3e98e85f54bfb613974c06ff6f35e5cd09
- 752b9fe24c357a04b0bdcad4d09e96bbad1bddfac8e637491b4181085eb58632
- 5c9cf2e4f2392a60cb7fe1d3ca94bda99968c7ee73f908dfc627a6b6d3dc404a
- ac95d34a008d0ec9deeb3d68afb16b2306a56b6bdc01810072a03b4f6a523586
- 273b91f37c01bd64d87c507db9868152665f964a2f5bbc744c207d6083e0af89
- dc9cbd484395367158c5819882ac811ee8464a62b018ffa51d3d476003643e54
- 57af8362ebba93155fb29af190fd450903bd62983179e5096cb24b5d0d1ea153
- 65267892a81d5e6c38c12d808623314ed9798156f3c24df2e8e906394fd51396

SHA1

- 2af5efccfbac6de50f0c48c1a232e0b4ce497538
- d5872e7c1c544fc5be51dc4aeb3e21af4f924928

- 34524fb4cc41a313604315c81da1a29fe8d2eeb7
- 54c74c995c734a59564de507c2608e0ecc5804f7
- ffb3cd3fb3ccb40352846ea5ece09e07767d6b5a
- dc5b5c9e991dffd1f692c052cf1a2af174b5f4b1
- afd3de962d53ee4caa94f67eeca62e0ecb369364
- 927e7b81816979c0393d926e013bb7b351756d43
- a9a282a11a97669d96cce3feaeaaa13051d51880

Source IP

- 5[.]181[.]156[.]84
- 95[.]179[.]252[.]217
- 136[.]244[.]67[.]59
- 45[.]61[.]138[.]170

Remediation

- Block the threat indicators at their respective controls.
- Do not download attachments from untrusted emails.
- Do not click on links provided in untrusted emails.
- Double-check a URL for spelling mistakes before entering credentials.
