Sodinokibi / REvil / Maze ransomware (TTPs & IOC)

blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html

We secured forensics evidence data in the form of disk images of VPS servers used by cybercriminals behind Sodinokibi / REvil ransomware (we also found Maze ransomware there):

- decryptor.cc
- dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion
- aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion

In this short post we would like to share information about their TTPs / tools with the community.

As an initial point of entrance attackers are exploiting Pulse Secure VPN vulnerability [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510].

On beforementioned VPS servers that were used to connect to the victims we found following tools:

- ADRecon [https://github.com/sense-of-security/ADRecon],
- CrackMapExec [https://github.com/maaaaz/CrackMapExecWin],
- ghost [https://github.com/ginuerzh/gost],
- impacket secretsdump [https://github.com/maaaaz/impacket-examples-windows/blob/master/secretsdump.exe],
- mimikatz [https://github.com/gentilkiwi/mimikatz],
- PentestBox with Metasploit [https://pentestbox.org],
- plink.exe [https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html],
- PowerSploit [https://github.com/PowerShellMafia/PowerSploit],
- Proxifier [https://www.proxifier.com],
- PsTools (PsExec)

URLs are collected from web browser history installed on the VPS machine.

They are also using two executables Eventlog-v6-fw3.exe (.NET 3) and Eventlog-v6-fw4.exe (.NET 4) that are transferred to the victim machines to view users login history (thx mak).

Eventlog-v6-fw3.exe
md5: 90ecf49afa94ffb47ffda283670366f3
sha1: 511a2d49df860ce260be59b308851c705816dc5f
sha256: 112e6ccb547d624e5c2ea7fb93065cf6681ee14f273b2a9968715b0db275a861

Eventlog-v6-fw4.exe
md5: 0bb3e286fcd2ecf1d62d515eb37c3f54
sha1: 452a53d70f89f97c1b0375f980223e460ead4901
sha256: 081bea740b6d6deb290b73ca8143967cd9815f5cc88d5d7f43d52b1a16823d93

peroxy.dll (Maze ransomware)
md5: 6d9134aaa7d3af23bd72e459414160a3
sha1: a7da29f84a8b9443479490538a131b9b90c08942
sha256: 745657e0c293a484aa85f0cf06f1281464e1b97e7610f5db50fb6219cad0c4ad

If you are victim of these attackers and observed connections from the following IP addresses:

- 37.1.203.158
- 37.1.204.143
- 5.45.87.6
- 93.190.142.7

Please contact us [https://redteam.pl/en/#contact].