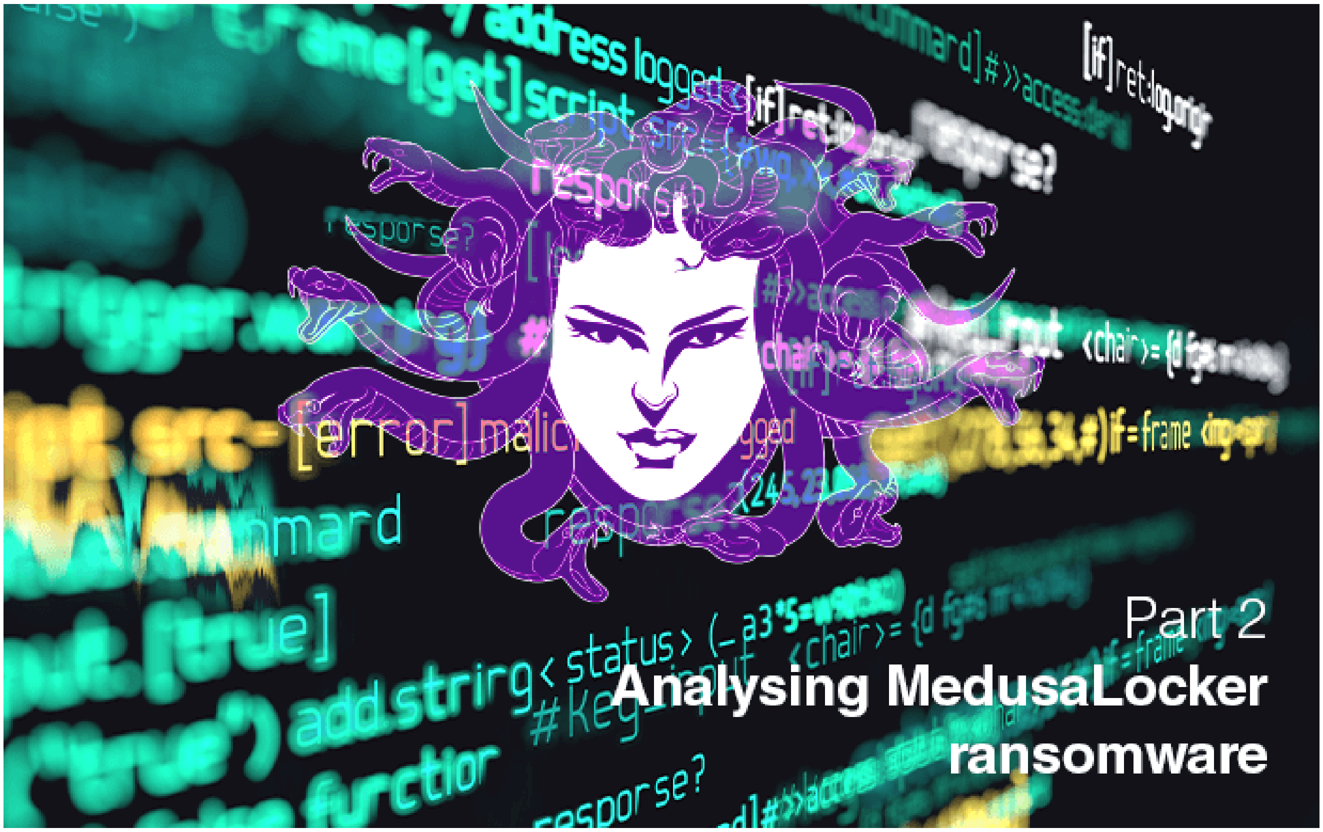
Part 2: Analysing MedusaLocker ransomware

theta.co.nz/news-blogs/cyber-security-blog/part-2-analysing-medusalocker-ransomware/



05/08/2020

(Part 2 of 3) In this 3-part post, we share the tradecraft from an RDP brute force linked ransomware event (MedusaLocker) we responded to in June 2020. We cover the business ramifications of the attack, technical analysis and some advice based on attacks such as these.

Continued from part 1...

Persistence

No specific persistence events were observed; it assessed that these intruders likely rely on tempo of operations and low-security posture of the victim to complete their objectives before being evicted.

Interestingly the earliest reference to the SVHOST task that executed the ransomware was at 16/06/2020 4:58:11 pm; even though most of the adversary activity was conducted later at 17/06/2020 3:00 to 4:00 am. This potentially represented a minimum viable (aka local) ransomware deployment in case the actors were detected and lost access to the host. Given the ~10hr time offset this may also represent a geographically distributed set of intrusion operators involved.

Privilege Escalation

The admin account compromised already had Domain Administer rights (T1110), so no privilege escalation was strictly necessary. Nonetheless, Theta observed the Domain\Administrator (S-1-5-21*domain*-500) account utilised by the intruder for lateral movement and reconnaissance. However, the exact mechanism these credentials were obtained with was not observed (other reporting suggests mimikatz staged in the `kamikadze` folder). Theta also observed the use of NT\SYSTEM (with C:\Windows\syswow64\config\systemprofile storing some useful artefacts).

Defense Evasion

Event logs and registry hives show artefacts related to the removal of ESET, the installed AV product on the server (T1089) before starting the encryption, some duplication of which may represent automated removal rather than by hand.

The previously mentioned arch.z$ sequence of files in the certutil log represents evidence of obfuscation of files or information (T1027), which is another technique to avoid detection.

Credential Access

Given the limited telemetry available, no evidence of Credential Access TTPs was observed (such as accessing system hives, the ntdis.dit file, or the ever-ubiquitous and suspected mimikatz).
While this was not necessary for the actors to carry out their objectives as referenced in the ***Privilege Escalation*** section, ultimately other accounts were obtained; however their mechanism for access remains unknown.

Recovered registry hives show the HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest key was set to 1; although given the age of the machine in question it was possible that the legitimate system administers never applied the fix to disable this. During the period the intruders were on the system there appeared to be a legitimate login from the Domain\Administrator account (S-1-5-21*domain*-500), which would have given an additional opportunity for the intruders to hijack these credentials, although this remains an open question.

Discovery

Several network discovery tools were used by the actor (T1018). Famatech’s *Advanced Port Scanner* was deployed to the host, with evidence suggesting interaction and use. The aforementioned *PSnmap.psd1* PowerShell datafile (likely an implementation of the wellknown nmap) is another network discovery/reconnaissance tool, and *2sys.ps1* script (if the same as referenced by Carbon Black) contains RDP scanning functionality.

The deployed binary *NetworkShare_pre2.exe* detected variously as *NetTool* has a diverse set of capabilities focused around network discovery. This was not removed from the staging directory unlike most of the other tooling across this intrusion.

WinPCAP 4.1.3 (rpcapd.exe) was also installed as a service onto the host by the actor, but its exact purpose cannot be inferred as it may be a dependency of other tooling used.

Lateral Movement

There is evidence from Security Event Logs of the Domain\Administrator account logging onto other hosts in the environment (via Event ID 4648). The connect-mstsc (*Connect-Mstsc.ps1)* likely provides RDP functionality in PowerShell.

All the other impacted hosts in the environment would not boot, so minimal forensic analysis was conducted into them as to the actions on them before encrypting. Other reporting details Medusa Locker spreading via PSexec and SMB - although with Domain Admin access a raft of lateral movement techniques is available.

Ultimately, the actors were able to spread their payload to effectively every host in the domain (bar a few off-site laptops).

Collection

There was no firm evidence of collection observed by the actor. Circumstantial evidence shows interaction with a SQL database present on the system.

Command and Control

As mentioned; the intruders logged in via RDP (External Remote Services - T1133) from **185.202.1[.]19, 213.7.208[.]69 & 5.2.224[.]56**.
Additional information, such as keyboard language or screen size was not available.

Exfiltration

The ransom note referenced potential data exfiltration and release, however no direct evidence of this was found and no effort was made to reach out and engage with the actor. Of the limited telemetry observed, there was a spike of 200Gb+ uploaded which did not match the pattern of life around the incident. If it was carried out, it may have been via RDPclip (Exfiltration Over Command and Control Channel - T1041) which would have left little evidence.

The actor has not followed up by engaging with the client. Access to this environment with Domain Admin would have given them enough access to harvest emails, and contact details for the business had they wished.

Impact

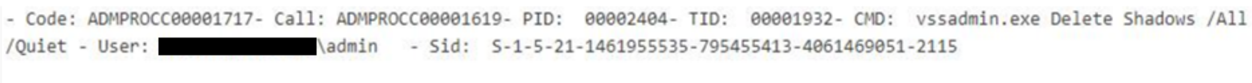
Given the nature of this intrusion, Data Encrypted For Impact (T1486) was the end goal. This was incredibly successful in this environment (see: *Headline Stats*).

The actor created a hidden scheduled task “svhost” (similarly named to the legitimate svchost process used by windows) and stored the binary in the %AppData%\Roaming\ folder for the compromised admin user. The binary itself was also named svhost.exe. The binaries contain a unique key per-campaign, so to preserve the confidentially of the client, this file won’t be made available in full.

Event logs show its execution every 15 minutes (this behaviour is consistent with other reported activity on Medusa Locker) as well as failure notices later on.

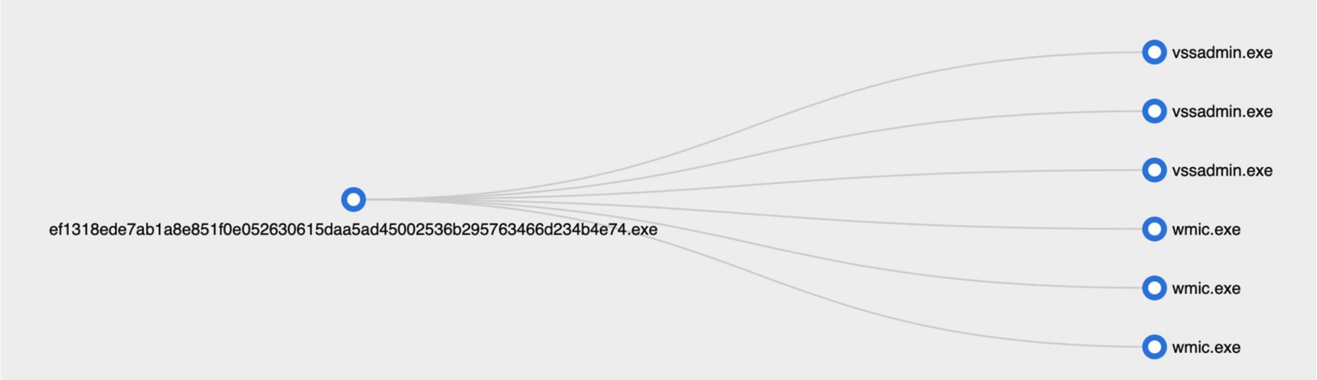
There remains some ambiguity around the exact timing of their operations. There’s evidence of the scheduled task running while the operators were still engaged on the host – unfortunately prefetch data was not available for analysis. Given the cryptographic overhead involved in sequentially encrypting each file on the file system, they may have been confident in the knowledge that the system would take some time to become fully degraded. Especially if the non-system drives were targeted first. There is some evidence (via event logs and shellbags) of graphical interaction with the Windows task scheduler to manipulate the scheduled task after it’s deployment – in what looks troubleshooting efforts.
It remains unclear if the operators intended to prevent the other hosts on the network from booting at all via encrypting the master boot record or if this was unintended - however, the result was that some of the machines were rendered inoperable - T1487 (Disk Structure Wipe).

A simple script named _*backup.bat* was used to delete Volume Shadow Copies – evidence of Inhibiting System Recovery (T1490) and this was executed on the system before encryption:

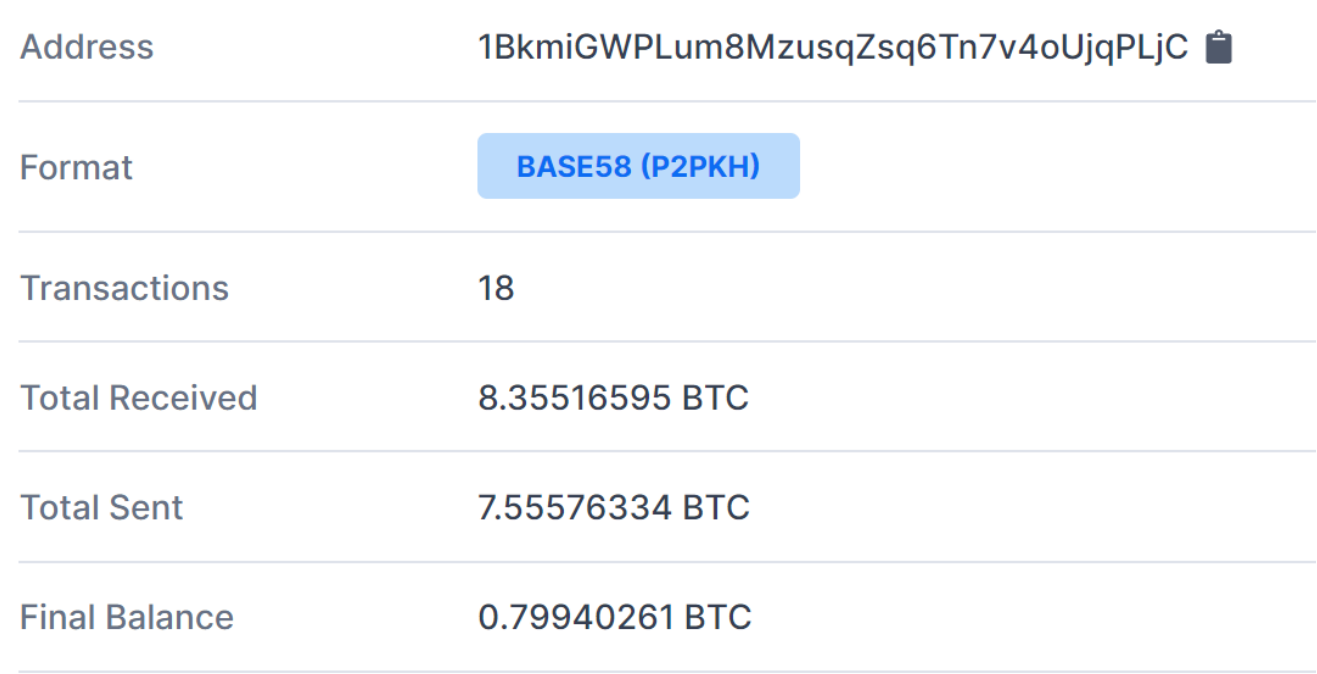


```
- Code: ADMPROCC00001717- Call: ADMPROCC00001619- PID:  00002404- TID:  00001932- CMD:  vssadmin.exe Delete Shadows /All
/Quiet - User: [redacted]\admin   - Sid:  S-1-5-21-1461955535-795455413-4061469051-2115
```

Other examples of MedusaLocker have shown vssadmin.exe to be spawned to further complicate recovery attempts (T1490):


ef1318ede7ab1a8e851f0e052630615daa5ad45002536b295763466d234b4e74.exe
vssadmin.exe
vssadmin.exe
vssadmin.exe
wmic.exe
wmic.exe
wmic.exe

The ransom demand pointed to a TOR address with a unique string for this campaign. While we did not interact with the attackers, others had, which in turn revealed a modestly successful return, at least for this campaign and further indirect evidence of this adversary successfully monetising their operation through Data Encrypted For Impact (T1486).



Address	1BkmiGWPLum8MzusqZsq6Tn7v4oUjqPLjC
Format	BASE58 (P2PKH)
Transactions	18
Total Received	8.35516595 BTC
Total Sent	7.55576334 BTC
Final Balance	0.79940261 BTC

Read part 3

Lead author: Hamish Krebs, Lead Consultant

Hamish has spent time across Australia and New Zealand responding to advanced threat actors; running large DFIR engagements in complex environments. He's also designed and deployed a variety of security solutions such as SIEMs and EDR suites across APAC.