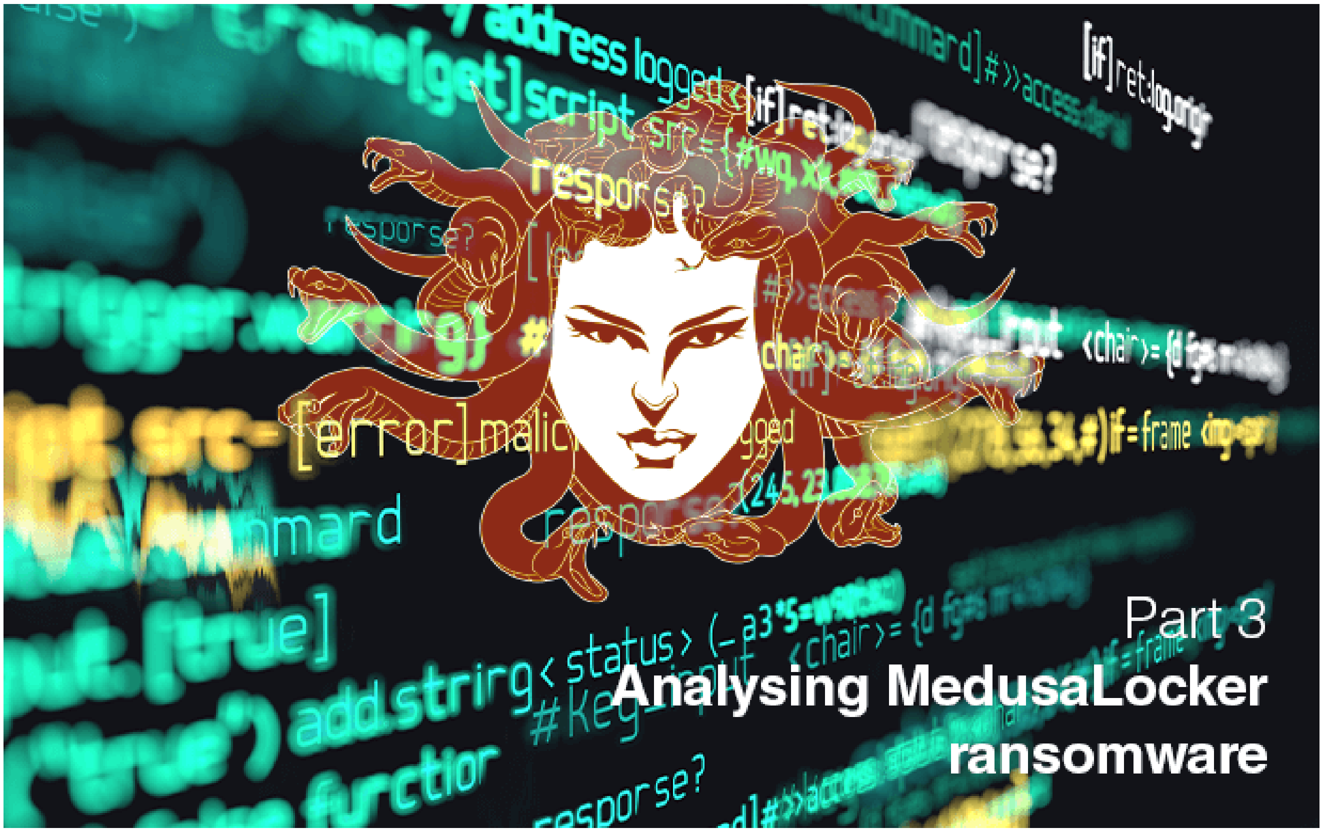
Part 3: analysing MedusaLocker ransomware

theta.co.nz/news-blogs/cyber-security-blog/part-3-analysing-medusalocker-ransomware/



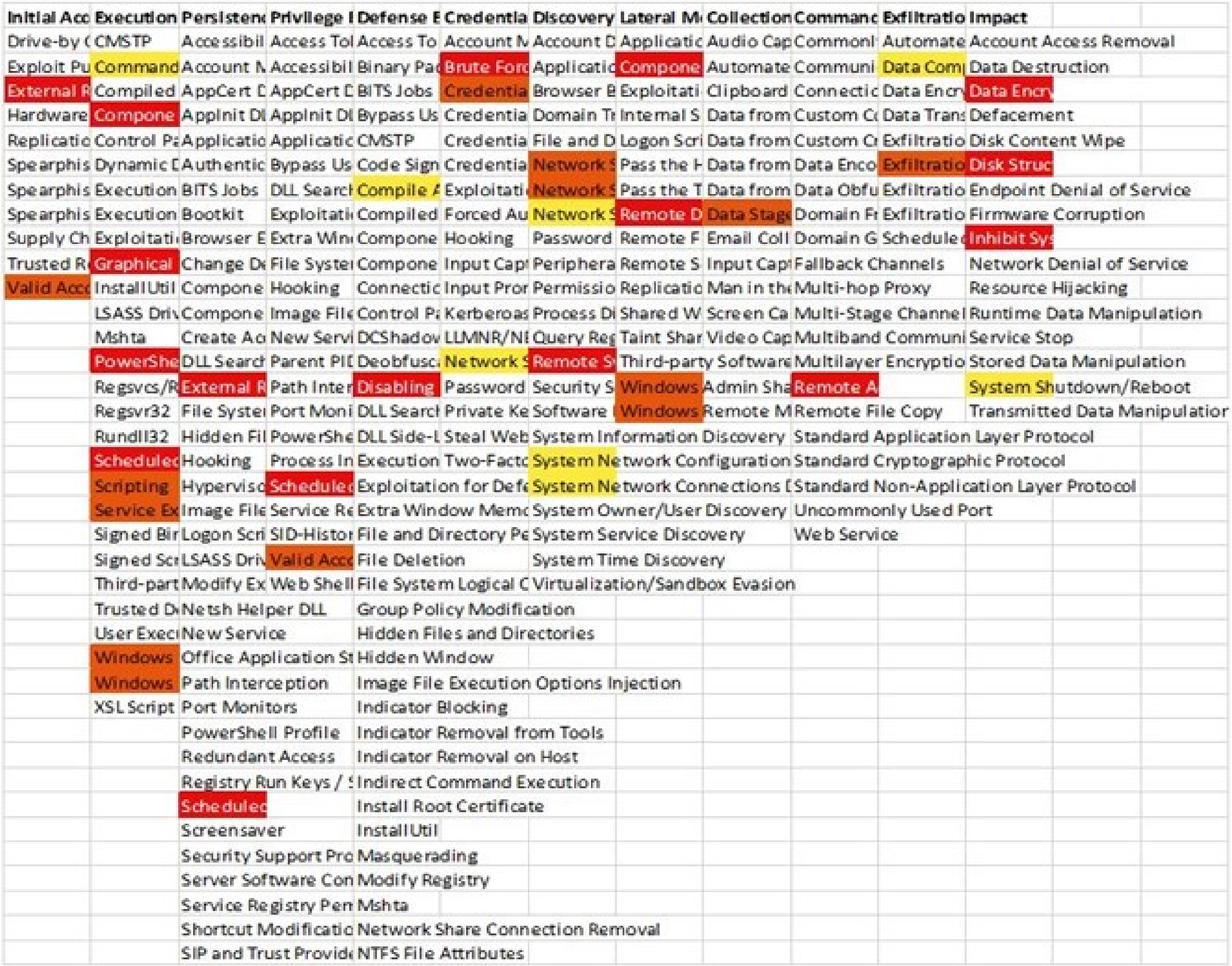
06/08/2020

(Part 3 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 parts 1 and 2...

ATT&CK Map

We have mapped the TTPs of this adversary to the MITRE ATT&CK framework as a heatmap of activity. We can see that this adversary used a limited, but powerful, selection of TTPs.



Initial Acc	Execution	Persistenc	Privilege I	Defense E	Credentia	Discovery	Lateral M	Collection	Commanc	Exfiltratio	Impact
Drive-by (	CMSTP	Accessibil	Access Tol	Access To	Account N	Account D	Applicatic	Audio Cap	Commonl	Automate	Account Access Removal
Exploit Pu	Command	Account N	Accessibil	Binary Pa	Brute Forc	Applicatic	Compone	Automate	Communi	Data Com	Data Destruction
External R	Compiled	AppCert D	AppCert D	BITS Jobs	Credentia	Browser B	Exploitati	Clipboard	Connectic	Data Encry	Data Encry
Hardware	Compone	AppInit DI	AppInit DI	Bypass Us	Credentia	Domain Tr	Internal S	Data from	Custom C	Data Trans	Defacement
Replicatio	Control Pa	Applicatio	Applicatic	CMSTP	Credentia	File and D	Logon Scri	Data from	Custom Cr	Exfiltratio	Disk Content Wipe
Spearphis	Dynamic D	Authentic	Bypass Us	Code Sign	Credentia	Network S	Pass the H	Data from	Data Enco	Exfiltratio	Disk Struc
Spearphis	Execution	BITS Jobs	DLL Search	Compile A	Exploitati	Network S	Pass the T	Data from	Data Obfu	Exfiltratio	Endpoint Denial of Service
Spearphis	Execution	Bootkit	Exploitati	Compiled	Forced Au	Network S	Remote D	Data Stage	Domain Fr	Exfiltratio	Firmware Corruption
Supply Ch	Exploitati	Browser E	Extra Win	Compone	Hooking	Password	Remote F	Email Coll	Domain G	Scheduled	Inhibit Sys
Trusted R	Graphical	Change De	File Syster	Compone	Input Cap	Periphera	Remote S	Input Cap	Fallback Channels		Network Denial of Service
Valid Acc	InstallUtil	Compone	Hooking	Connectic	Input Pror	Permissio	Replicatio	Man in the	Multi-hop Proxy		Resource Hijacking
	LSASS Driv	Compone	Image File	Control Pa	Kerberoas	Process Di	Shared W	Screen Ca	Multi-Stage Channel		Runtime Data Manipulation
	Mshta	Create Ac	New Servi	DCShadov	LLMNR/NI	Query Reg	Taint Shar	Video Cap	Multiband Communi		Service Stop
	PowerShe	DLL Search	Parent PID	Deobfusca	Network S	Remote S	Third-party Software		Multilayer Encryptio		Stored Data Manipulation
	Regsvcs/R	External R	Path Inter	Disabling	Password	Security S	Windows	Admin Sha	Remote A		System Shutdown/Reboot
	Regsvr32	File Syster	Port Moni	DLL Search	Private Ke	Software	Windows	Remote M	Remote File Copy		Transmitted Data Manipulatior
	Rundll32	Hidden Fil	PowerShe	DLL Side-L	Steal Web	System Information Discovery			Standard Application Layer Protocol		
	Scheduled	Hooking	Process In	Execution	Two-Facto	System Network Configuration			Standard Cryptographic Protocol		
	Scripting	Hypervisc	Scheduled	Exploitation for Defe		System Network Connections D			Standard Non-Application Layer Protocol		
	Service Ex	Image File	Service Re	Extra Window Memo		System Owner/User Discovery			Uncommonly Used Port		
	Signed Bir	Logon Scri	SID-Histor	File and Directory Pe		System Service Discovery			Web Service		
	Signed Scr	LSASS Driv	Valid Acc	File Deletion		System Time Discovery					
	Third-part	Modify Ex	Web Shell	File System Logical C		Virtualization/Sandbox Evasion					
	Trusted D	Netsh Helper DLL		Group Policy Modification							
	User Exec	New Service		Hidden Files and Directories							
	Windows	Office Application St		Hidden Window							
	Windows	Path Interception		Image File Execution Options Injection							
	XSL Script	Port Monitors		Indicator Blocking							
		PowerShell Profile		Indicator Removal from Tools							
		Redundant Access		Indicator Removal on Host							
		Registry Run Keys / S		Indirect Command Execution							
		Scheduled		Install Root Certificate							
		Screensaver		InstallUtil							
		Security Support Pro		Masquerading							
		Server Software Con		Modify Registry							
		Service Registry Pen		Mshta							
		Shortcut Modificatio		Network Share Connection Removal							
		SIP and Trust Provide		NTFS File Attributes							

Access PNG of image above.

Unfortunately, we're seeing the same TTPs being used over and over again for ransomware attacks, even if the initial access or lateral movement exploits vary.

We keep getting asked by customers to "tell us what we don't know about our vulnerabilities". While the use of traditional defensive frameworks like ISO 27001, NIST or PCI serve a compliance function, thinking like an attacker can rapidly highlight blind spots in your environment.

Phishing attacks are a nuisance but largely a means to an end for adversaries and won't put you out of business on their own. A ransomware attack will lose reputation, money and customers.
Never mind encrypting user workstations or file shares - destroying ERP and EDI systems (as happened here) will leave an organisation completely unable to trade and haemorrhaging money. That's not counting the cost of restoring business systems, which is incredibly labour-intensive, let alone the underlying IT infrastructure and the other parts of the Incident Response process, or the intangibles like the reputational damage.

Without enough cash reserves or insurance coverage, there’s a real chance of even medium-sized business ending up underwater depending on time-to-recovery and the bill at the end. You might be tempted to just pay the ransom – but this isn’t a great option either as there’s no guarantee you’ll get what you paid for. You still need to run through the IR (Incident Response) process to find the intruders and kick them out of your network.

We should also pause and take note of the human cost of these operations – they are brutal. The toll they take on those who suffer them is worse than intelligence motivated intrusions where “damage” is a more abstract concept. There is often a massive time crunch to restore systems at the expense of well-planned incident response process.

Indicators Annex

Strange Fruit
Several additional folders and files were deployed by the actor.
The following 4 deleted files were able to be recovered from the filesystem of the server with timestamps and other metadata suggesting they are associated with the actor. The purpose of these is not immediately clear and thus are not placed into this timeline.

EXPORT.EXE (35K) SHA256:
c945efb7f7c77cda9e54962b707268da57532ccd89253f0ccc98911cae7b3d77
PCC.EXE (512K) SHA256:
ef05323d278d60b3573c8d5b3bffd3a356eb4b8490c759ad71706e3e2eb9e470

PUZZLE.EXE (17K) SHA256:
aa49a4459cfd27cf4be40f8fa3bdabc198b93cb57f215aa61b28838af4b59005

RELAX.EXE (25K)
SHA256: 2d3b6ff5fc85f78dbe866d3a70a7f931f5d0b9007e4610310e603e6399f52665

Despite the naming convention they are not directly executable and appear to be obscured with high entropy values (> 7.99)

Other tooling

_backup.bat (SHA256:
465A1ACD9BE9B7BA027F34DFDF07C7A0ACEA6723F9D38A4E4CB920DC05425878)
NetworkShare_pre2.exe (SHA256:
47E3555461472F23AB4766E4D5B6F6FD260E335A6ABC31B860E569A720A5446)

ATT&CK Navigator Data

Protect your organisation with our help. Get in touch.

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.