

NetWalker Ransomware Group Enters Advanced Targeting “Game”

advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game

AdvIntel

May 19, 2020



BY BRIDGIT SULLIVAN
& DANIEL FREY



NetWalker now claims a singular preference for network infiltration, which is novel to the Russian-speaking ransomware community. As a result, the threat actor is requiring its new affiliates to have pre-existing access to large networks.

- o May 19, 2020
- o
- o 5 min read

Background and Summary

Throughout the COVID-19 crisis, there has been a drastic increase in the number of cyberattacks targeting the healthcare industry. The NetWalker ransomware syndicate is no exception to this trend. NetWalker responsible for such attacks as a high-profile ransom of the Australian transportation and logistics company Toll Group was first spotted in August of 2019. When it was discovered the group and the ransomware it used were originally referred by researchers as “MailTo.” However, it is the threat actor’s recent activity—not its origins—that has earned it recognition from the US Department of Homeland Security, the FBI, and the cyber community at large.

Within the past two months, NetWalker has become extremely active; the syndicate has revolutionized the way it conducts business by transitioning to a network intrusion-focused, Ransomware-as-a-Service (RaaS) model. This new business model allows NetWalker to collaborate with other seasoned cybercriminals who already have access to large networks and have the ability to disseminate ransomware.

NetWalker distributes ransomware via two main methods: 1) phishing schemes & spam emails; and 2) large-scale network infiltration. NetWalker now claims a singular preference for network infiltration, which is novel to the Russian-speaking ransomware community. As a result, the threat actor is requiring its new affiliates to have pre-existing access to large networks.

Once deployed, NetWalker ransomware quickly encrypts the user’s files and presents the victim with this ransom note:

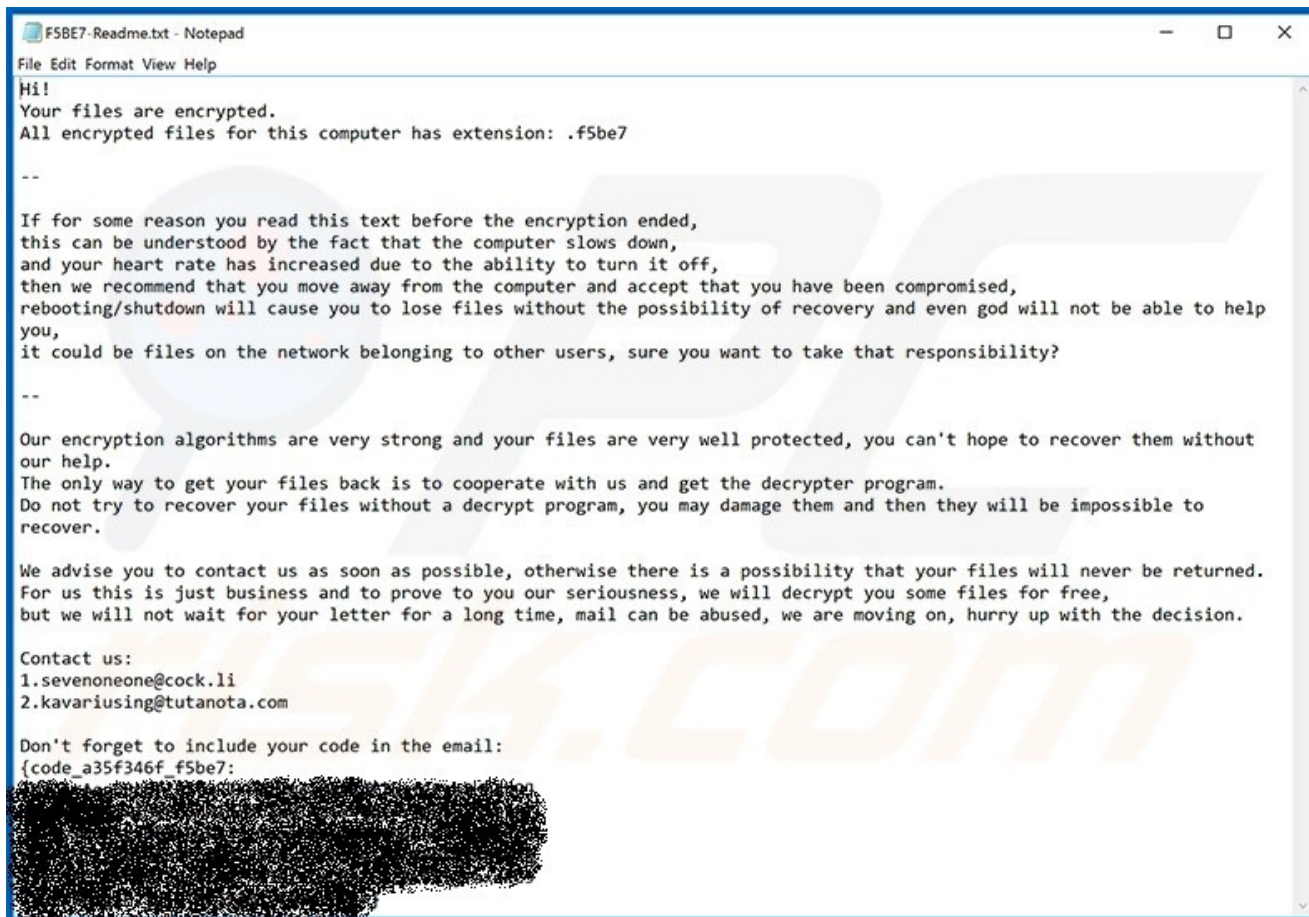
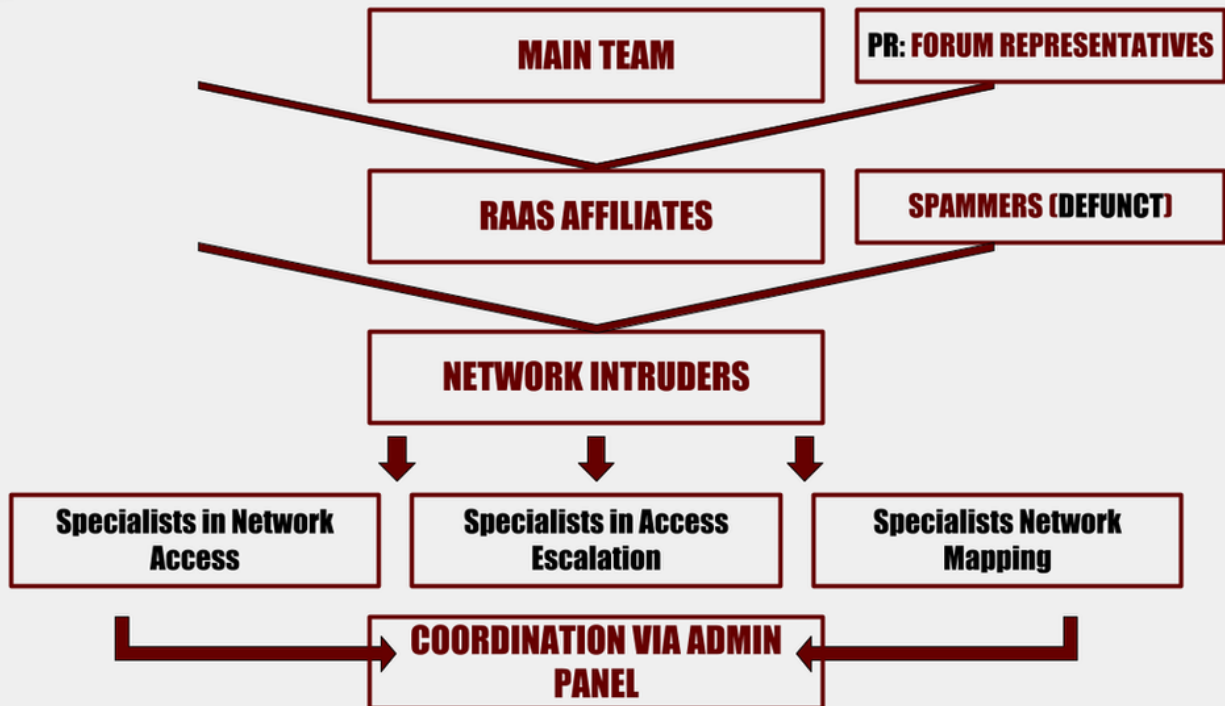


Image 1: NetWalker ransom note (source: PC Risk)

In addition to increasing its manpower and expanding its capabilities, NetWalker has been actively taking advantage of the COVID-19 crisis. The threat actor's phishing emails have contained an attachment titled "CORONAVIRUS_COVID-19.vbs," which targets people who are interested in learning more about the crisis, as well as individuals and entities involved in the healthcare industry. NetWalker poses a significant threat, as it has been carrying out these high-profile attacks while simultaneously posting on the top-tier Russian-language DarkWeb forums in order to expand its operations and capabilities.

NETWALKER STRUCTURE



Assessment and Findings

On March 19, 2020, NetWalker representatives on forums began to propagate the announcement of the ransomware affiliate program. The phrasing and the context of these as well as further announcements shed light on the internal workings of this group. Notably, the Representative expressed a preference for affiliates “who prioritize quality, not quantity.” The threat actor’s preference for quality stands in stark contrast to other Russian-speaking actors’ ransomware operations, which often focus instead on mass production and brute force attacks. In addition, the NetWalker team offered the following victim-focused material as incentives for potential affiliates: IP addresses, access to domain administrator accounts, network-attached storage (NAS) access, organization name, and organization revenue.

byte
●

B

Seller
● 0

Posted March 19

We are announcing the hiring of adverts [affiliates] for processing [disseminating ransomware] via networks and spam. We are interested in people who prioritize quality, not quantity. We give preference to those who can work with large networks and have their own material [network access]. We will recruit a limited number of affiliates until we fill all the vacancies. We are offering you a fast and flexible locker, a convenient admin panel in TOR, and an automatic service. Access to the service is through crypt files from AV. We give the verified adverts formatted, ready-to-go material (ip \ account of the domain admin \ access to nas \ information about AV \ organization name \ revenue) for processing networks. The locker has been working since September 2019 and has proved itself, it cannot be decrypted. You will receive all the detailed information about the locker and working conditions via PM [private message] after compiling the application.

Application Form:

- 1) What area do you work in.
- 2) Your experience. Which affiliate programs have you worked with and what was your profit.
- 3) How much material do you have and when are you ready to start, how much material [network quantity and scale] do you plan to process.

Image 2: NetWalker centers their operations around network compromise. The group references access to corporate networks as “materiel” and explains in detail how exactly the skill and knowledge of network intrusion will fit into their operations.

A month after the RaaS program was advertised, on April 19, 2020, NetWalker clarified its affiliate requirements, claiming interest only in experienced, Russian-speaking network intruders—not spammers—with a preference for immediate, consistent work. Traditionally, cybercrime organizations have used tactics, techniques, and procedures (TTPs) such as mass phishing campaigns to gain control over targeted networks, which has oftentimes created an opportunity for amateur hackers to get involved. However, as the group has continuously outlined in their posts, NetWalker is behaving differently. The collective is selectively choosing the affiliates it collaborates with, creating an exclusive group of top-tier network intruders to execute its new RaaS business model.

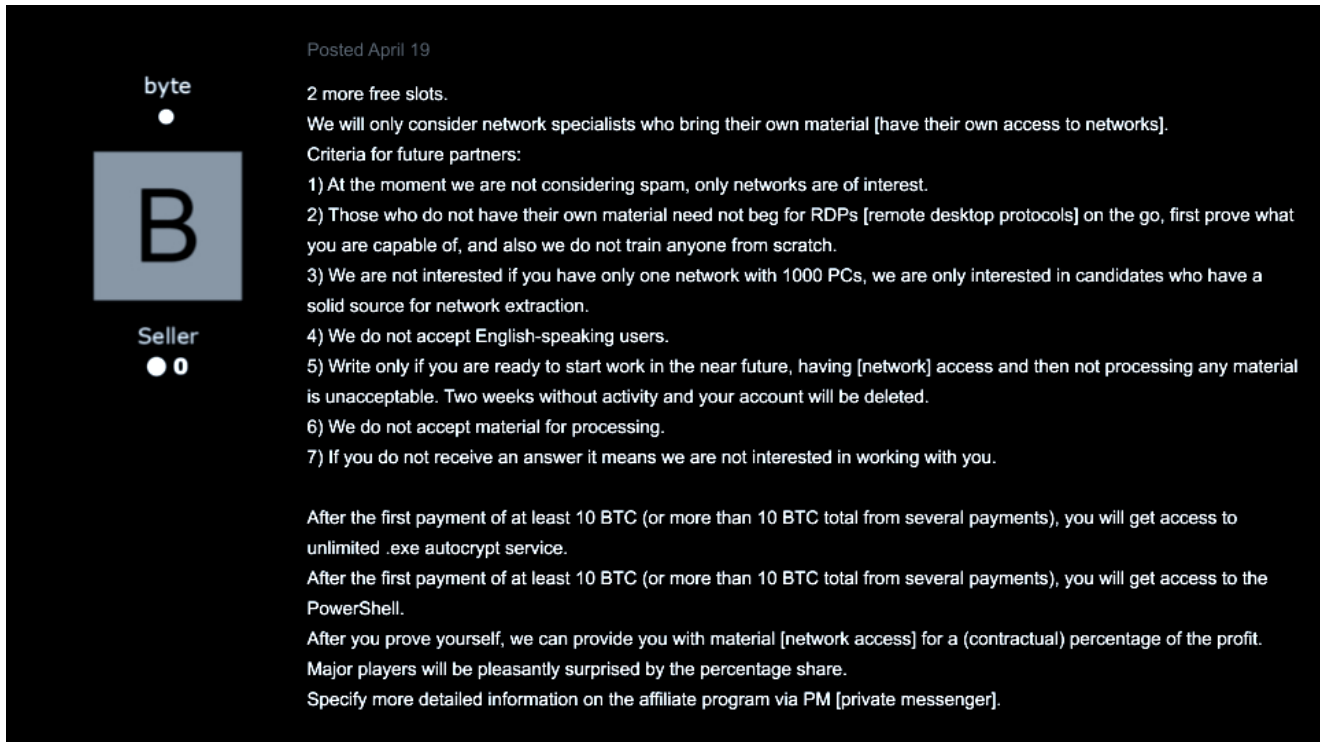


Image 3: NetWalker follows the trends established by REvil across the Russian-speaking cybercrime community - to pursue highest standards and rigid requirements for the RaaS candidates

According to AdvIntel's sensitive source intelligence, after a potential candidate passes the review by group members, they receive the following note, detailing NetWalker's operational code for affiliates.

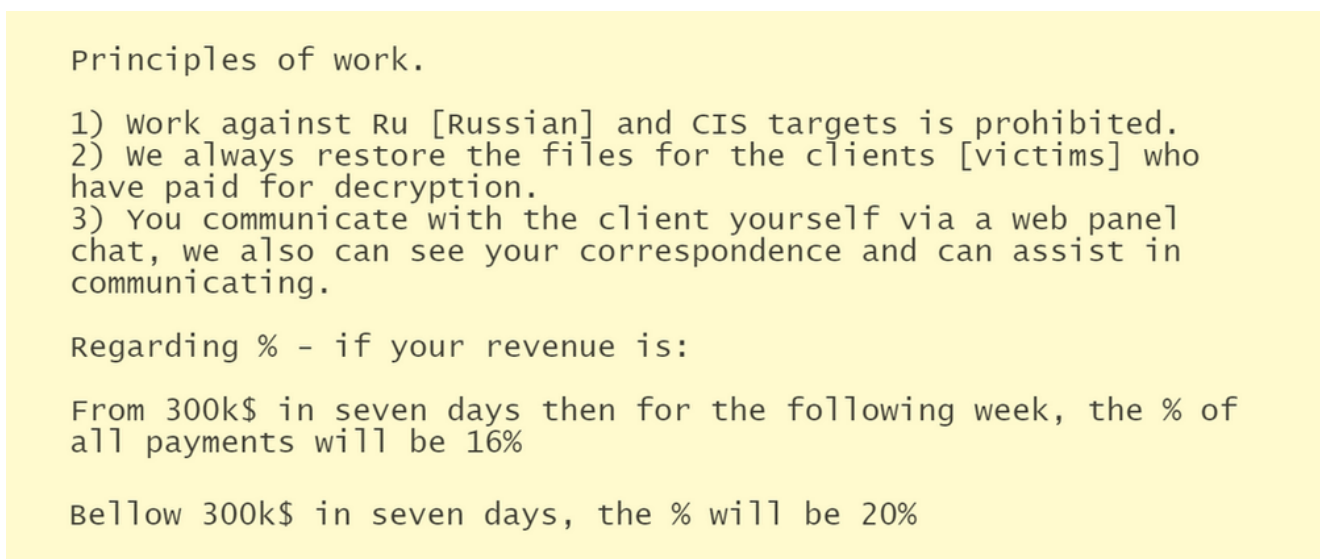


Image 4: Translation from Russian - segments in brackets refer to the translator's comments

What is especially noteworthy is NetWalker's guarantee of providing decryption to the victims when the ransom is paid. Additionally, the group's percentage share - 20% to 80% (with 20% for the NetWalker and 80% for the affiliate) can be considered very generous. To compare, GandCrab offered 30/70 or even 40/60 shares.

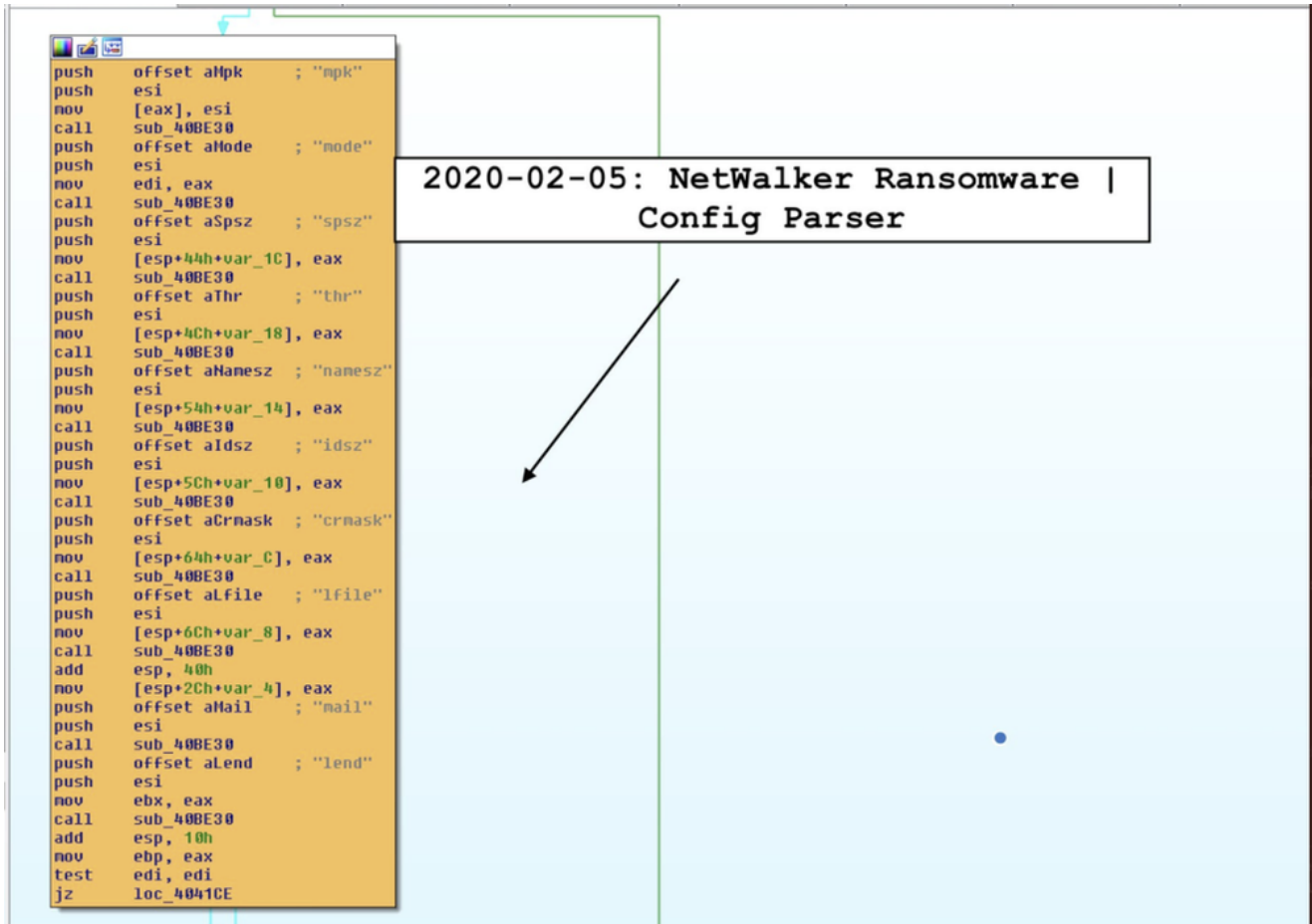


Image 5: NetWalker ransomware includes a modular configuration setting.

00403B5E	. 83C4 1C	ADD ESP,1C	
00403B61	. 85C0	TEST EAX,EAX	
00403B63	. 74 1F	JE SHORT 00403B84	sdsa.00403B84
00403B65	. 56	PUSH ESI	
00403B66	. E8 65000000	CALL 00403B00	sdsa.00403B00
00403B6B	. 8B00 0011410	MOV ECX,DWORD PTR DS:[4111A0]	
00403B71	. 83C4 04	ADD ESP,4	
00403B74	. 85C0	TEST EAX,EAX	
00403B76	. BA 01000000	MOV EDX,1	
00403B7B	. 0F45CA	CMOVNE ECX,EDX	
00403B7E	. 8B00 0011410	MOV DWORD PTR DS:[4111A0],ECX	
00403B84	> 55	CALL EBX	
ESP=0012FF5C	2020-02-05: NetWalker Ransomware Config Parser		
Address	ASCII dump		
00619A95	C{"npl":"ExgCIpycIjzspm07Loi9L5u0cxC+Uz/HjxlfOn7UqUE=","node":0,"		
00619AE5	thz":"1500,"spsz":16384,"namesz":6,"idsz":5,"ormask":"","mailto:(m		
00619B25	ail1)),cid":"","mail":["		
00619B65	.com"},"file":"","(ID)-Readme.txt","lend":"","SGkhD0pZb3UyIGzpb6UzIGF		
00619B85	yZSBIBnNyeX80ZM0uD0pBb6wzW5jcnIwdGUKIGzpb6UzIGzvo iB0aG1zIGNvXB		
00619BEE	1dGUYIghoyBleHRlbnNpb24lC57alR900oNCi0tD0oNClzIGzvo iBzb21IHJ		
00619C25	lVY0IvbIB5b3UgonUhZCB0aG1zIHRleH0gYnVub3JlIHRoZSBIBnNyeX80a19uIGU		
00619C65	uzGVLARkqGpoyBjVW4gVnUgdW5kZUJzdG9vZCBleSB0aG1zIGzvo iB0aG1zIGNvXB		
00619C95	oZSBjB2lwdXRo iBzb693oyBkb3duLCANCrFuZCB5b3UyIGh lVY0IHJhZGUGaG9		
00619CE5	zIGlUyY3JlVWZlZCBkMjUgdG9gdGhIGF iaklpdHkqdg9gdHJybiBpdCBvZnVzD0p		
00619D25	0aG0uIHd1IHJlV29tblUuzCB0aG1zIGzvo iBzb21IHJlV29tblUuzCB0aG1zIGz		
00619D65	toH0ZXiGyW5kIGFjV2UudCB0aG1zIHRoYX0gonUz0G9vZ2l iaklpdHk/D0oNCi0tD0o		
00619D95	sD0pyZlUJvb3Rpbmco2h1dG9vZ2l iaklpdHk/D0oNCi0tD0oNCi0tD0oNCi0tD0o		
00619DA5	0yB3aXRob3U0IHRoZSBub3NzalkUpbG18eSBvZiByZWVudnUyeSBhbn0gZkZlbiB		
00619E25	nb20gd2l iaklpdHkqdg9gdHJybiBpdCBvZnVzD0p0aG1zIGzvo iBzb21IHJlV29tblUuz		
00619E65	pb2UyIGzvo iBzb21IHJlV29tblUuzCB0aG1zIHRoYX0gonUz0G9vZ2l iaklpdHk/		
00619E95	yZSB5b3Ugd2FudCB0aG1zIHRoYX0gonUz0G9vZ2l iaklpdHk/D0oNCi0tD0o		
00619EE5	NCK91o iBIBnNyeX80a19uIGFz29yaXRob3UyIGh lVWZlZCBkMjUgdG9gdGhIGF		
00619F25	zSB5UyIGzpb6UzIGFyZSB2ZUJzdG9vZCBleSB0aG1zIGzvo iB0aG1zIGNvXB		
00619F65	wZSB0yByZWVudnUyIHRoZlW0gd2l0aG91dCBvZnVzD0p0aG1zIGzvo iBzb21IHJlV29tblUuz		
00619FA5	heSB0yByZWVudnUyIHRoZlW0gd2l0aG91dCBvZnVzD0p0aG1zIGzvo iBzb21IHJlV29tblUuz		
00619FE5	zIGFuZCBnZlW0gdGhIGRlV3JlZ0Rl iBuon9nconFtLg0KR68gn90IHRySB0yBy		
0061A025	yZlWVudnUyIHJlV29tblUuzCB0aG1zIHRoYX0gonUz0G9vZ2l iaklpdHk/D0oNCi0tD0o		
0061A065	1IG1hSBkVM1hZUgdGh lB5b3UyIGzpb6UzIGFyZSB2ZUJzdG9vZCBleSB0aG1zIGNvXB		
0061A095	zSB0yByZWVudnUyLg0K0pZSBhZHZpc2UgeW91HRvIGVudnUyeSBhbn0gZkZlbiB		
0061A0E5	yo29vbiBhoyBub3NzalkJz2Swgb3R0ZUJ3aX0hIHRoZUJlIGl zIGEgoG9vZ2l iaklp		
0061A125	pdHkqdg9gdHdCB5b3UyIGzpb6UzIHdpbGwgnV2ZlIGVnUgonU0dXJuZlW0pG9vZ2l		
0061A165	gd90gdGpoyBjVW4gVnUgdW5kZUJzdG9vZCBleSB0aG1zIGzvo iB0aG1zIGNvXB		
0061A195	yIHNIonlvDNUz0hZlCB3ZSB3alKsIGRlV3JlZ0Rl iBuon9nconFtLg0KR68gn90IHRy		
0061A1E5	yIGzpb6UzIGFyZSB2ZUJzdG9vZCBleSB0aG1zIGNvXB0aG1zIGzvo iB0aG1zIGNvXB		
0061A225	vo iBIBnNyeX80a19uIGFyZSB2ZUJzdG9vZCBleSB0aG1zIGNvXB0aG1zIGzvo iB0aG1zIGNvXB		
0061A265	nIG9vLCB0dXJyeSB1oCB3aX0hIHRoZlW0gd2l iaklpdHk/D0oNCi0tD0oNCi0tD0o		
0061A295	6D0oLnttVl iaklpdHkqdg9gdHdCB5b3UyIGzpb6UzIHdpbGwgnV2ZlIGVnUgonU0dXJuZlW0pG9vZ2l		
0061A2E5	kZSB5b3UyIGzpb6UzIGFyZSB2ZUJzdG9vZCBleSB0aG1zIGNvXB0aG1zIGzvo iB0aG1zIGNvXB		
0061A325	["system volume information","*windows.old","*:*\\users**temp		
0061A365	","*nsocache","*:*\\winnt", ".*windows.us", ".*perflogs", ".*		
0061A395	boot","*:*\\windows", ".*:\\program file\\vmware", ".*\\		
0061A3E5	users**temp", ".**winnt", ".**windows", ".*\\pro		
0061A425	gram file\\vmware", ".*appdata\\microsoft", ".*appdata\\packages",		
0061A465	,".*microsoft\\provisioning", ".*dvd maker", ".*Internet Explorer",		
0061A495	,".*Mozilla", ".*Mozilla", ".*Old Firefox data", ".*\\program file*		
0061A4E5	\\windows media", ".*\\program file\\windows portable", ".*windo		
0061A525	ws defender", ".*\\program file\\windows nt", ".*\\program file\\		
0061A565	windows photo", ".*\\program file\\windows side", ".*\\program f		
0061A595	ile\\windows powershell", ".*\\program file*ouass", ".*\\progr		
0061A5E5	am file\\microsoft games", ".*\\program file\\common files\\sys		
0061A625	ten", ".*\\program file\\common files\\shared", ".*\\program file		
0061A665	\\common files\\reference ass", ".*\\windows\\cache", ".*tempor		
0061A695	y internet", ".*media player", ".*:*\\users*\\appdata*\\microso		
0061A6E5	ft", ".**\\users*\\appdata*\\microsoft", "file":["ntuser.		
0061A725	.dat", ".*iconcache.db", ".*gdipfont*.dat", ".*ntuser.ini", ".*usrclass.dat"		
0061A765	,".*usrclass.dat", ".*boot.ini", ".*bootmgr", ".*bootnt", ".*desktop.ini",		
0061A795	.*ntuser.dat", ".*autorun.inf", ".*ntldr", ".*thumbs.db", ".*bootsect.bak", ".*b		
0061A7E5	ootfont.bin"], "ext":["nsp", ".*exe", ".*sys", ".*nsc", ".*nod", ".*clb", ".*mli",		
0061A825	.*regtrans-ms", ".*theme", ".*hta", ".*shs", ".*nonedia", ".*diagpkg", ".*cab", ".*los		
0061A865	",".*msstyles", ".*cux", ".*drv", ".*lons", ".*diagofg", ".*dll", ".*ock", ".*lnk", ".*loo		
0061A895	",".*ldx", ".*ps1", ".*npa", ".*opl", ".*lcl", ".*msu", ".*nsl", ".*nls", ".*scr", ".*adv", ".*3		
0061A8E5	86", ".*com", ".*hlp", ".*non", ".*lock", ".*386", ".*wpk", ".*anl", ".*pff", ".*rtp", ".*idf"		
0061A925	[".**.*diagcab", ".*cab", ".*epi", ".*deskthemepack", ".*bat", ".*themepack"]		

Image 6: NetWalker ransomware includes a detailed configuration.

On May 10th, the group posted another request for affiliates, this time asking specifically for “experienced networkers with their own material.” The Representative claims that the ransomware “works on all Windows” operating systems from Windows 2000 onwards; the actor also claims that NetWalker not only encrypts network assets using a customizable, multi-threaded locker but also maps the breached networks, including resources such as

NAS. As for the architecture of the ransomware itself, the Representative has explained that “the locker is located inside a [PowerShell] script,” which circumvents the need to upload the payload to an external network. NetWalker claims that this feature helps “deal” with antivirus products, including Windows Defender.

Exfiltrating Corporate Data

Notably, the NetWalker claims the ability to exfiltrate data and publish it to a “blog.” This is a significant assertion, given both the credibility of the threat actor and the consequences this action could pose to entities that possess confidential or sensitive information. The group’s representative has backed up its claim with links to the aforementioned blog. They also bolstered its credibility with screenshots of payouts it has received from its extortion efforts.

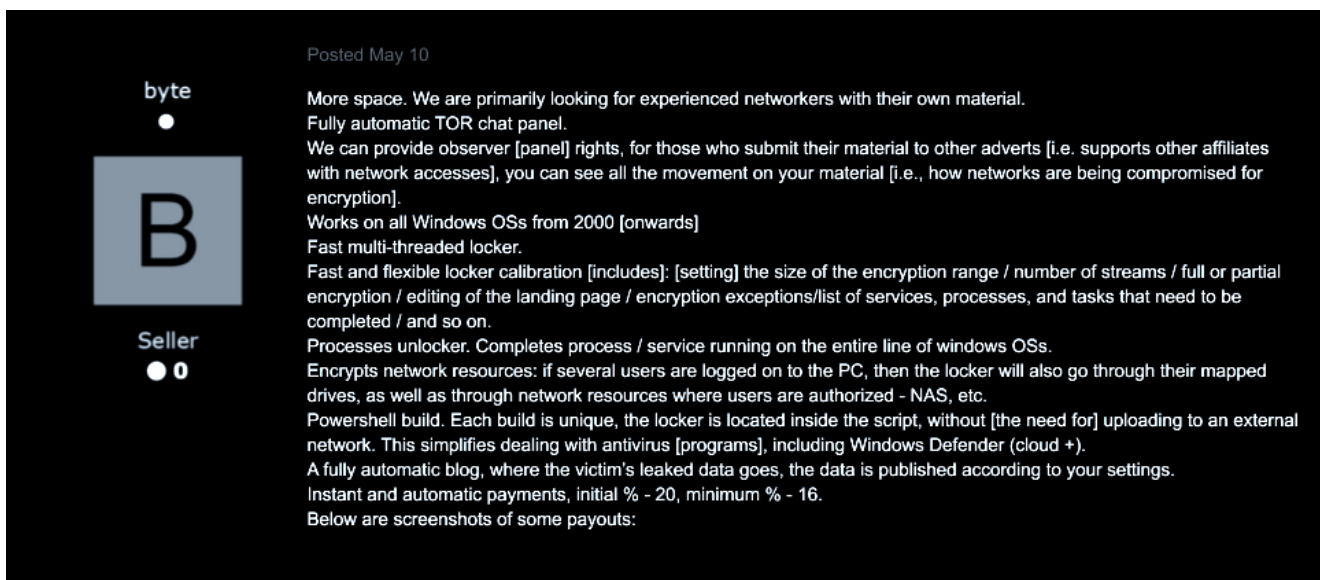


Image 7: Besides the description of the locker’s capabilities, this post provides valuable insights on how the network compromise processing is integrated into the workflow of the ransomware operations



39NRnZ... \$1,038,491.70 

3DJqpb3V4LTK... \$47.01 

+\$1,038,491.70



3L4AW5... \$696,073.29 

3Fw5meZ6y4P... \$3.20 

+\$696,073.29



3DW3ijP8nziQ... \$76.34 

3JHTYZ... \$1,506,415.29 

+\$1,506,415.29



39aovz... \$1,457,666.31 

+\$1,457,666.31

Image 8: Screenshots offered by NetWalker illustrate the scale of their operations

On May 13th, the Representative posted another update with references to targeted entities; most importantly, the post also included a link to the blog in which those entities' data have been exfiltrated to.

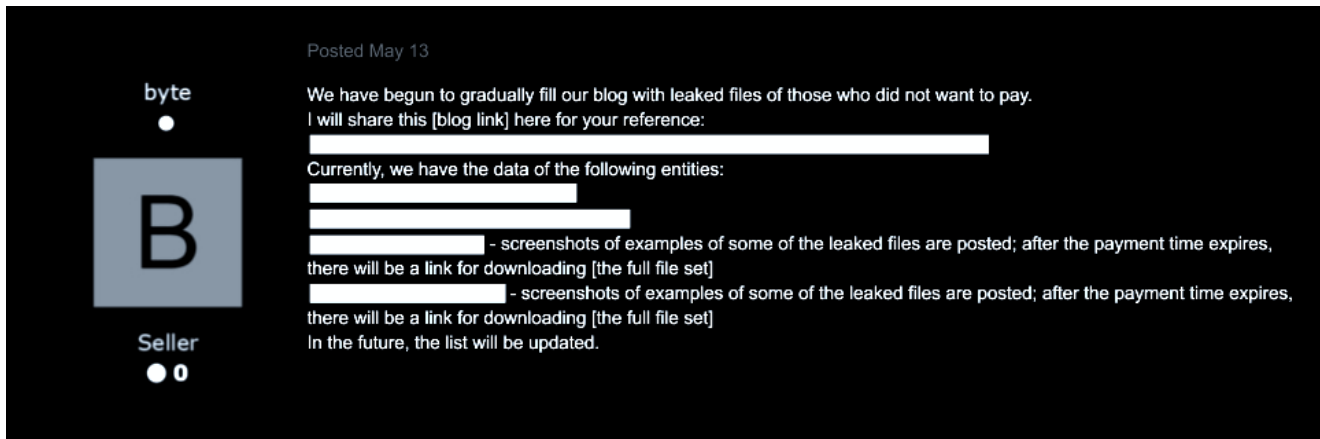


Image 9: Judging from the existence of this blog, the actor's threat to exfiltrate and publish victims' data appears highly credible.

Conclusion

Not only is NetWalker actively expanding its operations, but the group is also changing the way ransomware is deployed. The group's activities on top-tier DarkWeb forums also provide a unique insight into the current workings of the ransomware ecosystem. Traditionally, Russian-speaking ransomware groups have focused on the mass production of phishing emails and spam. Over the past two months, however, NetWalker has detailed its ideal affiliates: experienced network intruders, specifically those who speak Russian. This transition to network intrusion as the main method of ransomware dissemination is a novel concept within the Russian-speaking ransomware community.

Over the past two months, NetWalker has proven its legitimacy through notorious attacks and the ability to provide unique, victim-focused material to its affiliates. The syndicate has also proven willing and able to exfiltrate victims' data to a DarkWeb blog. In addition, the size of the ransom payments it has posted is significant, ranging from hundreds of thousands to millions of dollars. NetWalker is a rapidly evolving, credible actor that poses a significant threat, especially to the healthcare industry during the COVID-19 crisis. It is likely that there will be more updates from, and attacks by, NetWalker in the weeks and months to come.

Yara Signature: NetWalker Ransomware

```
rule crime_win32_netwalker_1 {
```

```
meta:
```

```
description = "Detects Netwalker Ransomware Variant"
```

```
author = "@VK_Intel"
```

```
reference = "https://twitter.com/VK_Intel/status/1240767289793929217"
```

```
date = "2020-03-19"
```

```
strings:
```

```
$str1 = "unlock"
```

```
$str2 = "spsz"
```

```
$str3 = "onion"
```

```
$start_code = {e8 ?? ?? ?? ?? 85 c0 74 ?? e8 ?? ?? ?? ?? 85 c0 74 ?? e8 ?? ?? ?? ?? 85 c0  
74 ?? e8 ?? ?? ?? ?? e8 ?? ?? ?? ?? 6a 01 8b ?? ?? ?? ?? ?? ff d0 6a 01 ff ?? ?? ?? ?? ??  
33 c0 c2 10 00}
```

```
condition:
```

```
( uint16(0) == 0x5a4d and
```

```
( 3 of them )
```

```
) or ( all of them )
```

```
}
```

Advanced Intelligence, LLC, thanks Bridgit Sullivan and Daniel Frey for contributing to this investigation.