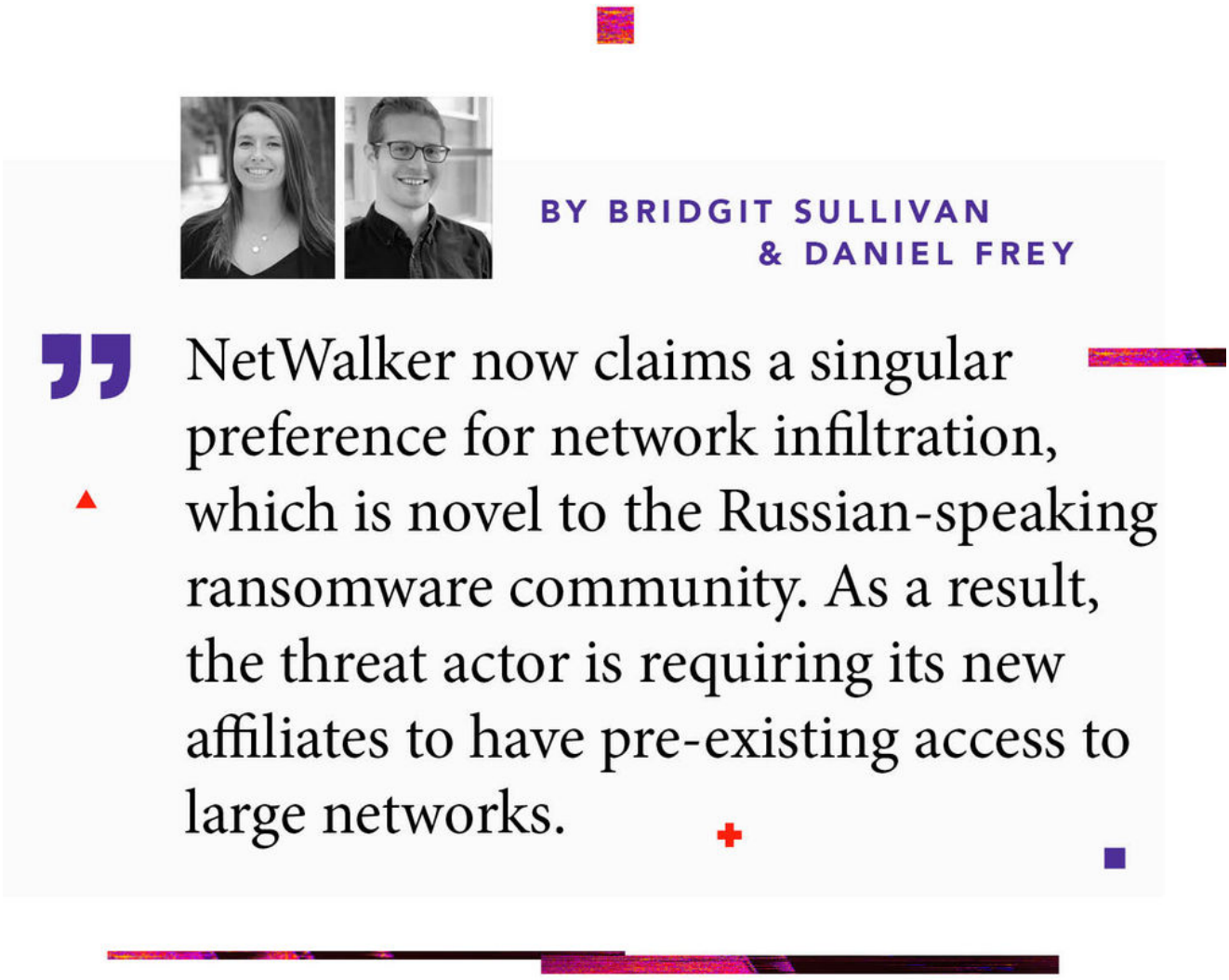
# NetWalker Ransomware Group Enters Advanced Targeting “Game”

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

AdvIntel May 19, 2020




- May 19, 2020
- 
- 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:

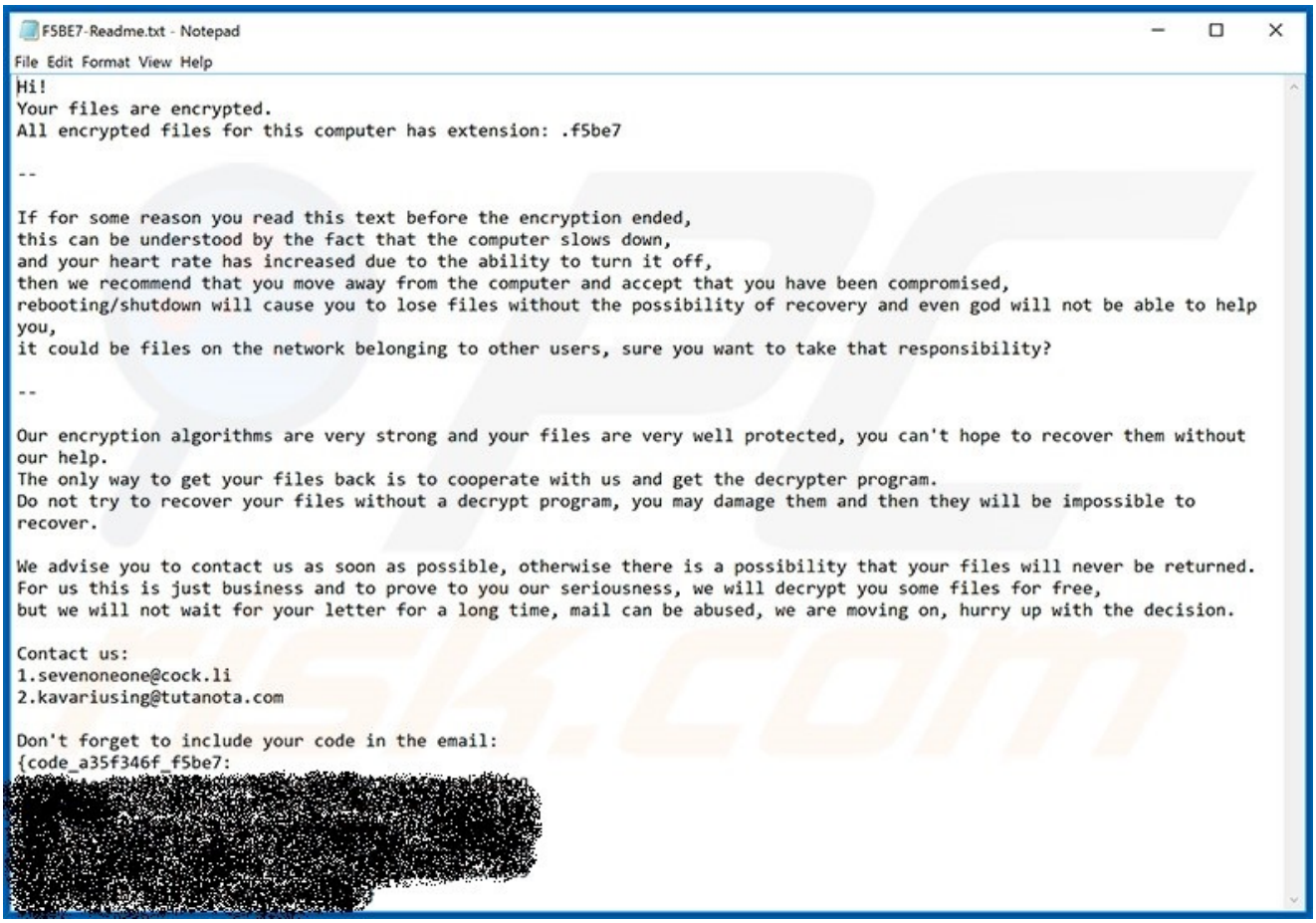
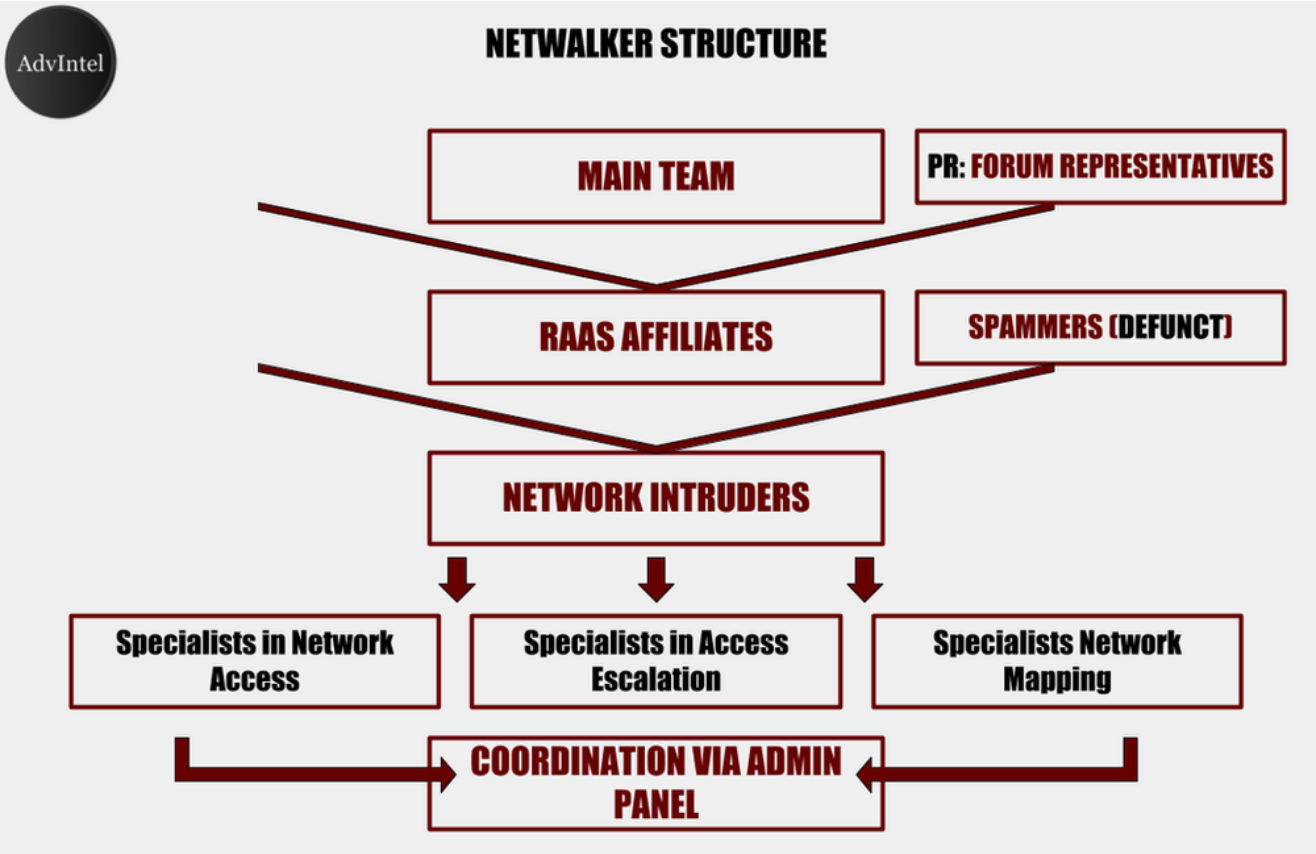


*Image 1: NetWalker ransom note (source: PC Risk)*

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.




**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.

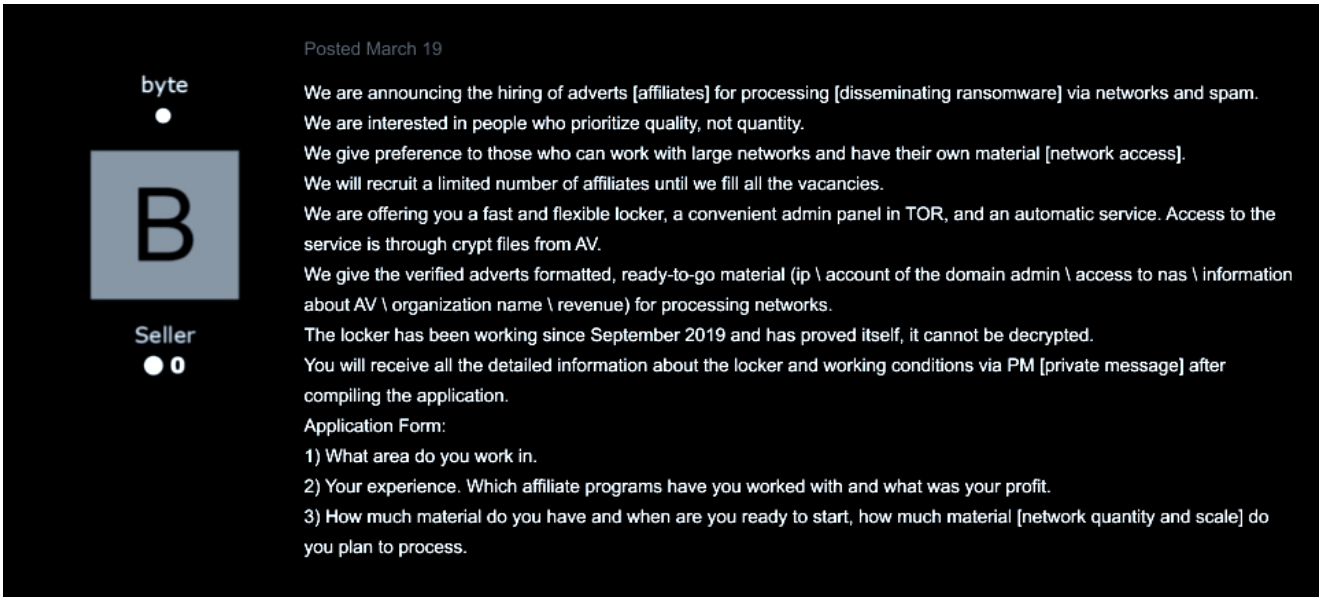



*Image 2: NetWalker centers their operations around network compromise. The group references access to corporate networks as "materiel" and explains in detail how exactly the skill and knowledge of network intrusion will fit into their operations.*

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.

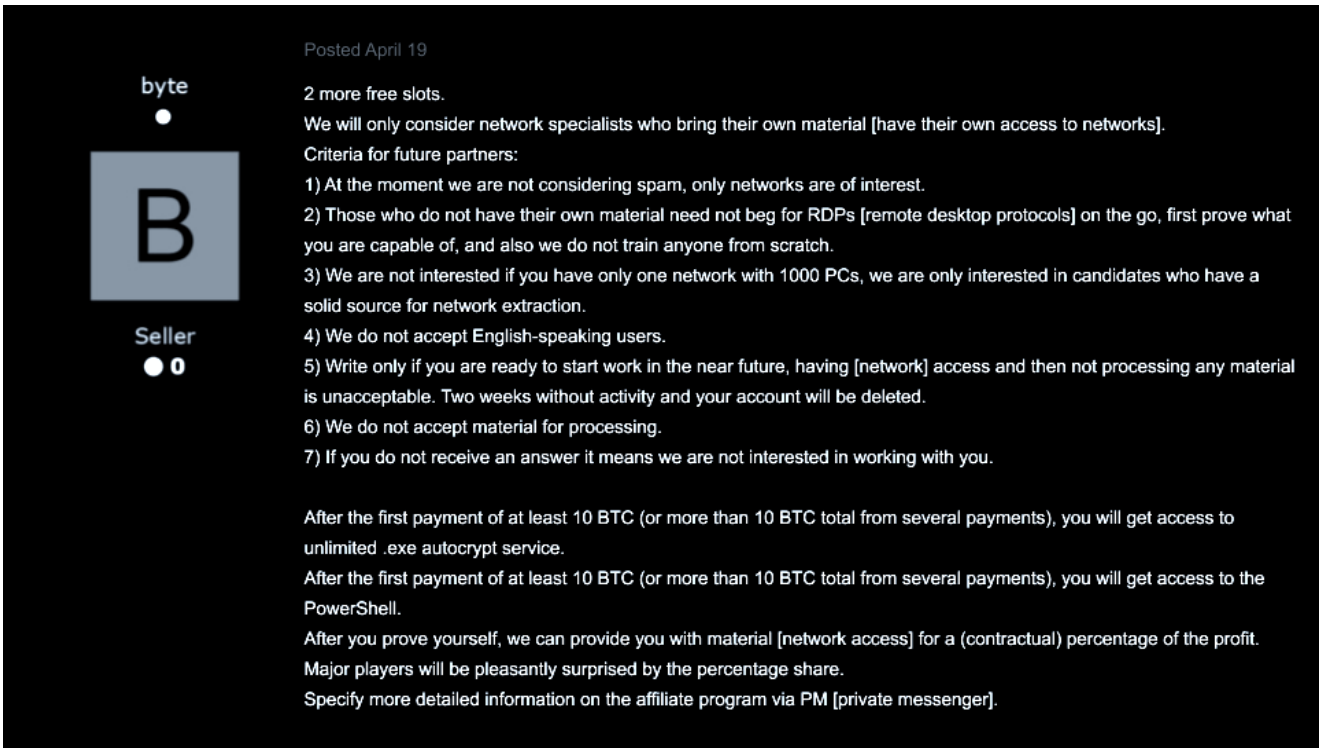



*Image 3: NetWalker follows the trends established by REvil across the Russian-speaking cybercrime community - to pursue highest standards and rigid requirements for the RaaS candidates*

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.

```
Principles of work.

1) Work against Ru [Russian] and CIS targets is prohibited.
2) We always restore the files for the clients [victims] who
have paid for decryption.
3) You communicate with the client yourself via a web panel
chat, we also can see your correspondence and can assist in
communicating.

Regarding % - if your revenue is:

From 300k$ in seven days then for the following week, the % of
all payments will be 16%

Bellow 300k$ in seven days, the % will be 20%
```

*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.

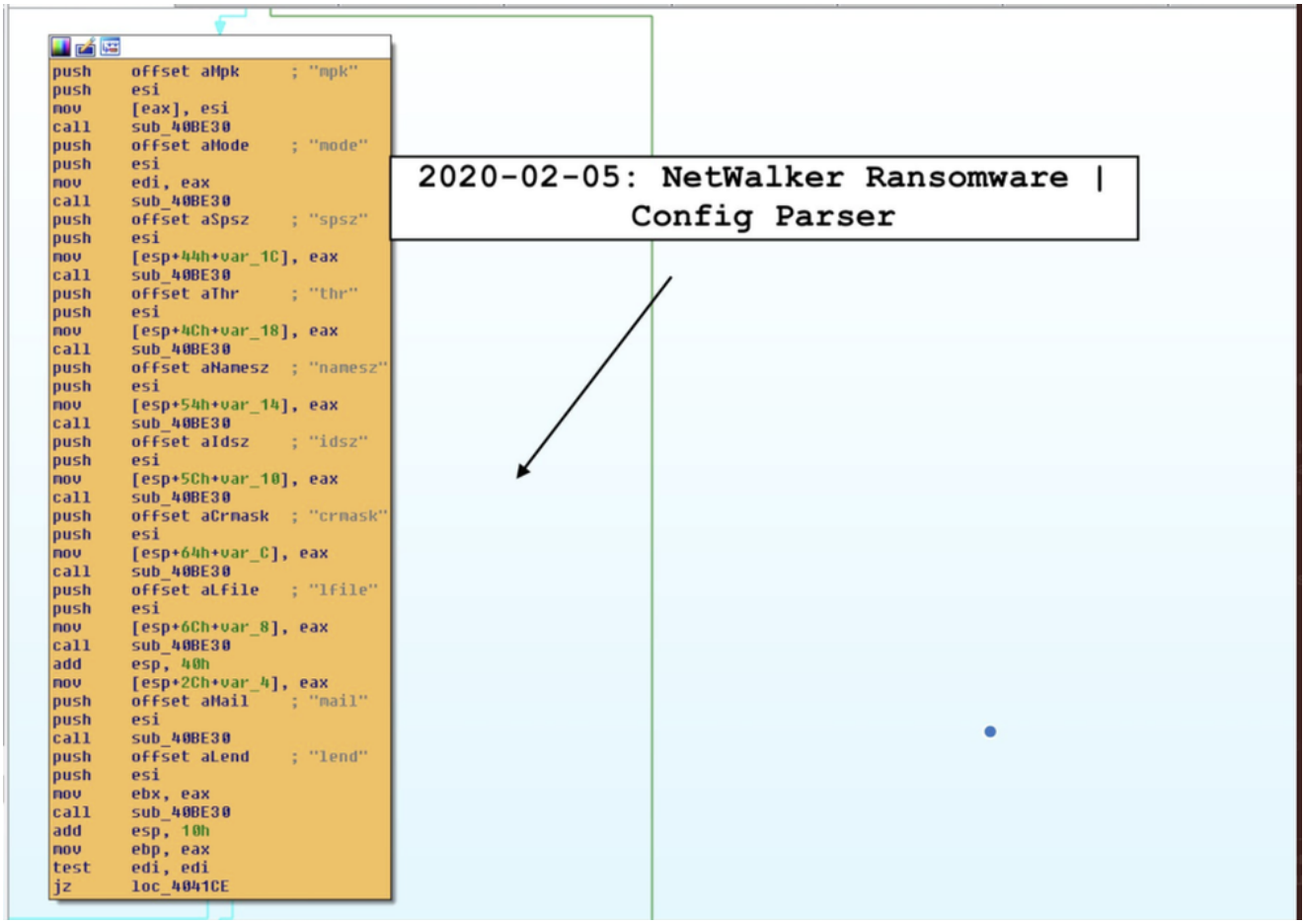


*Image 5: NetWalker ransomware includes a modular configuration setting.*

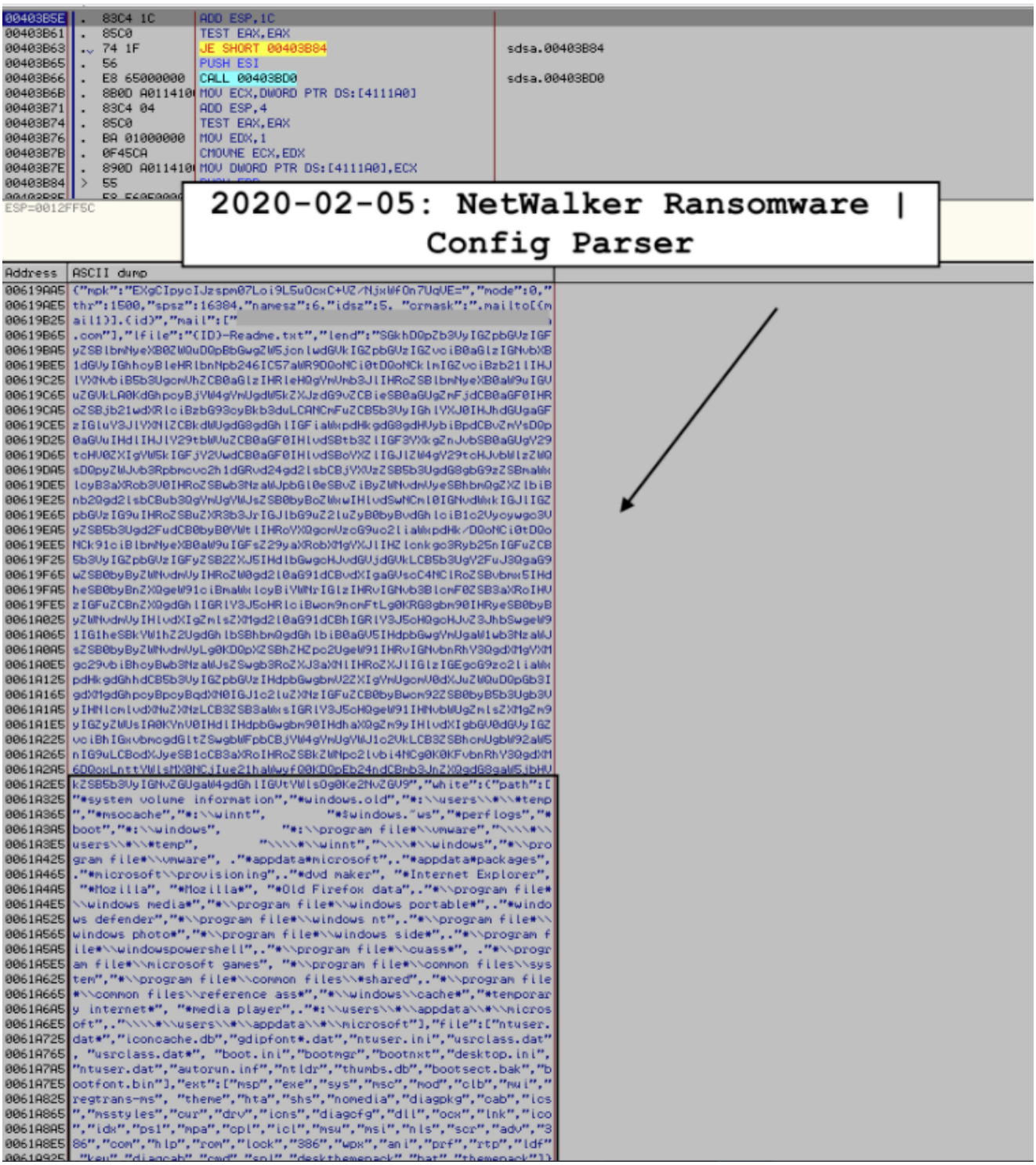



*Image 6: NetWalker ransomware includes a detailed configuration.*

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.

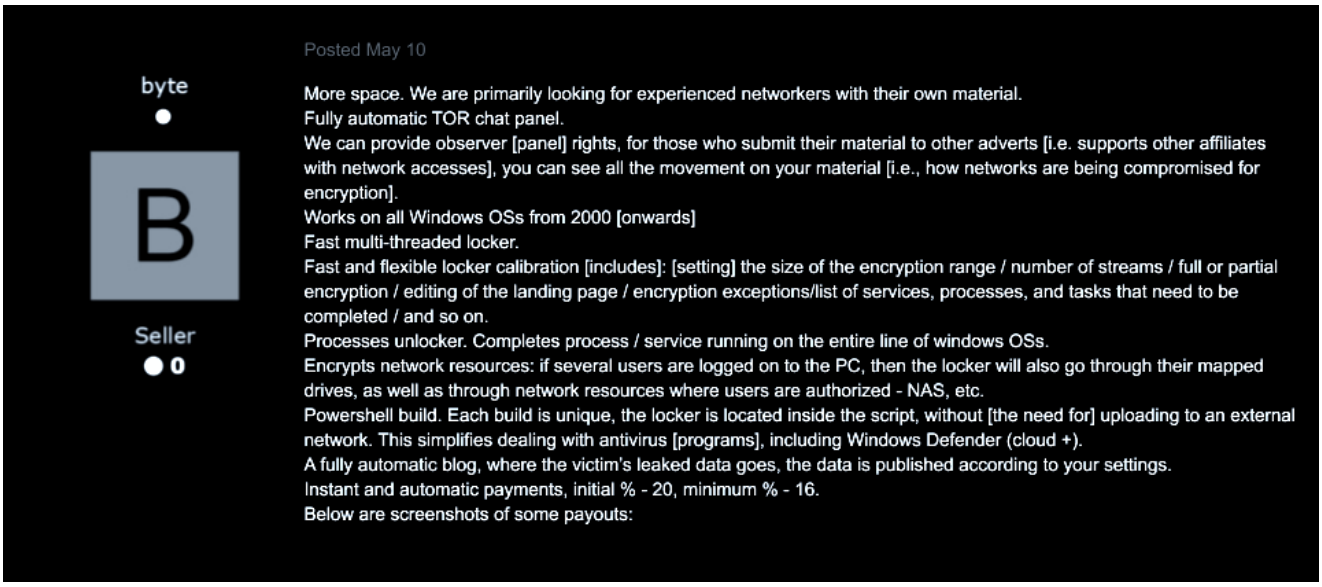


*Image 7: Besides the description of the locker's capabilities, this post provides valuable insights on how the network compromise processing is integrated into the workflow of the ransomware operations*

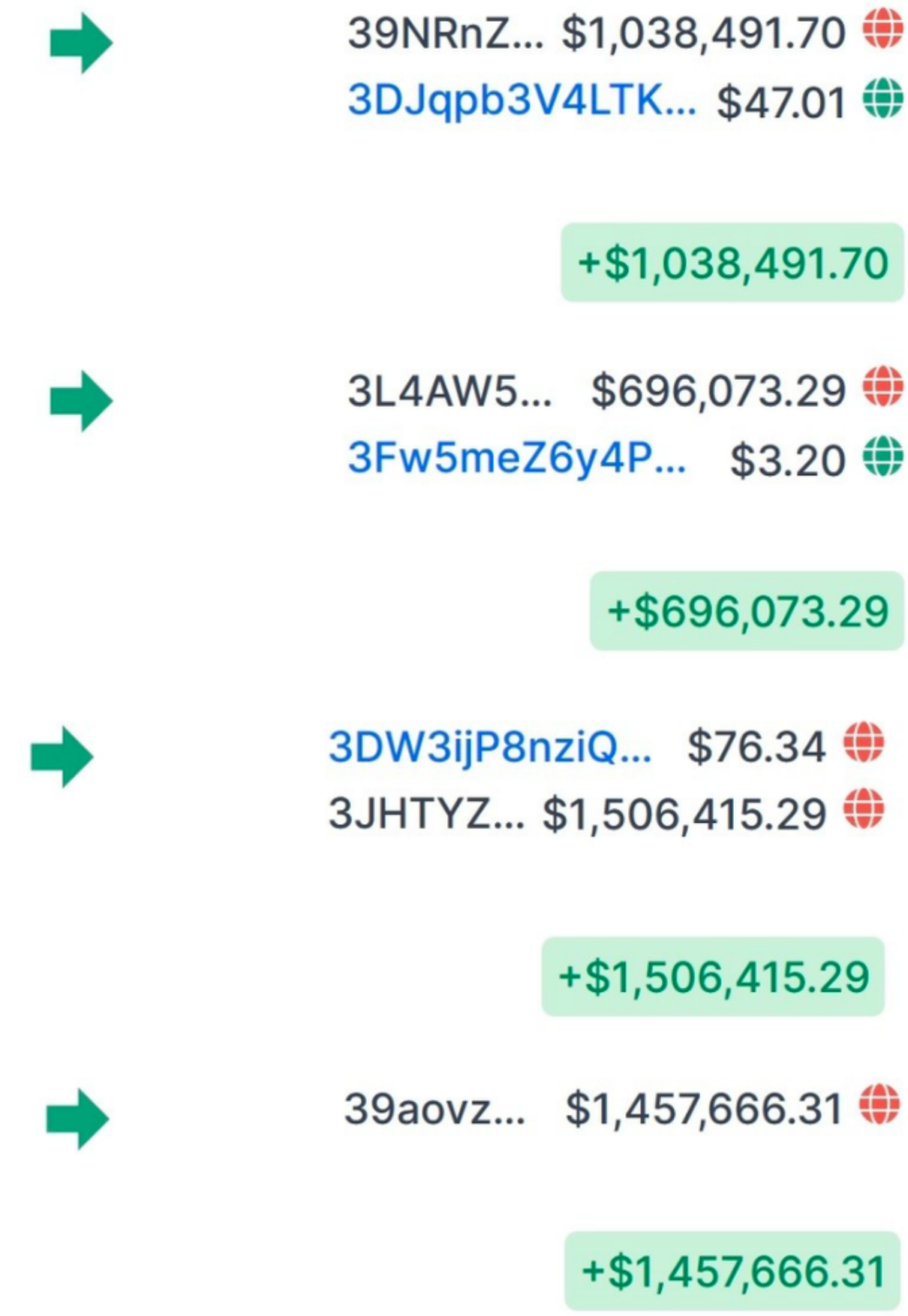



*Image 8: Screenshots offered by NetWalker illustrate the scale of their operations*

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.

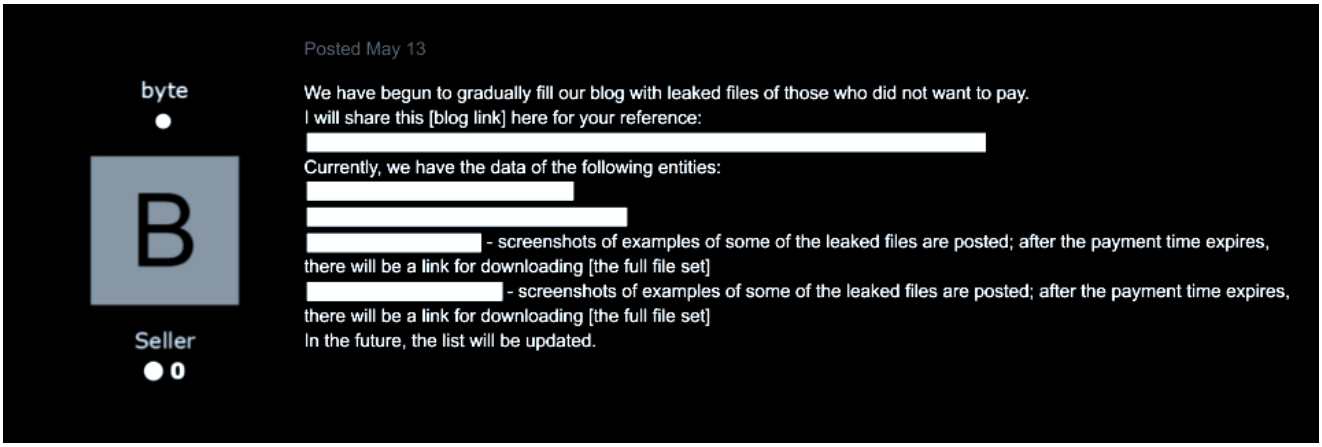


*Image 9: Judging from the existence of this blog, the actor's threat to exfiltrate and publish victims' data appears highly credible.*

**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.*