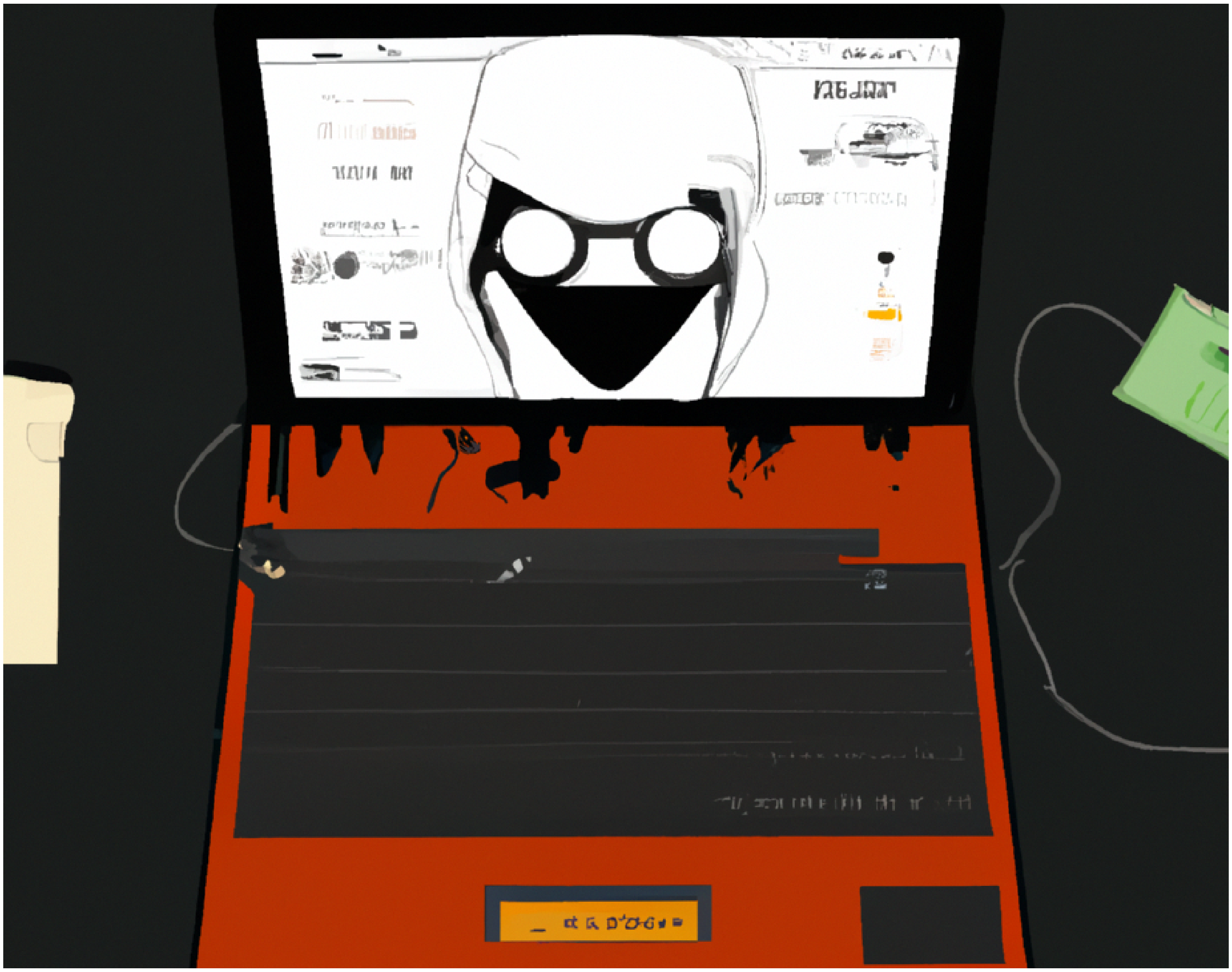
Lighting the Exfiltration Infrastructure of a LockBit Affiliate (and more)

medium.com/@lcam/lighting-the-exfiltration-infrastructure-of-a-lockbit-affiliate-and-more-f57fbb7a4e79

L M

October 4, 2023



L M

--

Executive Summary

- We investigated a recent LockBit extortion incident that occurred in Q3 2023, which involved an unusual FTP server located in Moscow. The hostname of this server was identified as matching many hostnames found in various posts on the LockBit leak site.

- Our investigation revealed that this remote endpoint is associated with criminal activities dating back to 2019, indicating that these hosts were likely under the control of the same technical administration.
- Furthermore, the results of our analysis also linked this particular hostname to an individual named “Bentley,” who was previously the technical lead and system administrator for the Conti group.
- Based on our findings, we identified a potential connection between a person responsible for maintaining these hosts and both the LockBit incident and a broader spectrum of criminal activities.

NOTE: This version of the report has been redacted for TLP:WHITE disclosure.

Introduction

Digging into ransomware infections always provides valuable insights. This time, we investigated peculiar details of a recent Lockbit-based intrusion that happened in Q3 2023, and we uncovered connections between a wide range of cybercriminal activities, highlighting some of the constants characterizing a dangerous threat actor operating deeply in the digital underground.

In this article, we present our findings from examining the exfiltration infrastructure associated with one of the most notorious LockBit affiliates, which has also been tracked by CISA. We elucidate how these findings are interconnected within a broader threat landscape encompassing numerous other criminal business verticals, all seemingly under the control of a single enigmatic administration.

Technical Details

Evidence from the field

At some point, the Lockbit incident investigation landed at a very interesting point: the ransomware affiliate conducted the data exfiltration phase through an FTP channel tunneled over a TLS connection. As reported by CISA in their “AA23–165A” joint advisory back in June 2023, the operator ingeniously exploited the FileZilla FTP client and employed Ngrok tunneling services to facilitate this process. Notably, in this specific instance, the ransomware affiliate utilized a server located in Moscow, which was administered by a Hong Kong-based hosting provider known as Chang Way Technologies Co. Limited.

A quick examination of the publicly accessible profile of the Moscow-based server swiftly uncovered a peculiarity. Among the array of exposed services, there was an active RDP (Remote Desktop Protocol) service running on the machine, disclosing not only its operating system version but also, of greater interest, its hostname.

Figure. The hostname of a LockBit exfiltration server

At first sight, the particular hostname does not mean much: the format “WIN-XXXXXXXXXXX” resembles the typical default, randomly generated hostname chosen by the Windows operating system during the installation phase. But here we noticed the interesting part: multiple past LockBit victims show this hostname within their dedicated page on the gang’s data leak site. This re-use might not be just aesthetic, the chance of multiple LockBit affiliates randomly matching their hostname is almost zero, so this correlation enables us all to spot the connection between this particular affiliate and its victims.

Figure. Example of a LockBit victim showing the “WIN-LIVFRVQFMKO” hostname.

In addition, the machine presenting this hostname presents the system language configured to the Russian one, but this is not the only interesting fact. Pivoting on the infrastructure we found 105 hosts with the same hostname serving an IIS-based FTP service. Such servers have been deployed in 16 countries spread worldwide: Russia, Netherlands, Finland, United States, Kazakhstan, Turkey, Ukraine, Czech Republic, Latvia, Norway, Poland, Romania, Uzbekistan, Germany, France, and Greece.

Figure. Remote Desktop login screen of “WIN-LIVFRVQFMKO”

Widening the Connections

After the discovery of this hidden connection, we moved forward to investigate what else could be linked to this LockBit affiliate through its infrastructure, and was astonishing: many researchers were stumbling up into that hostname for various malicious operations. For instance:

- In September 2019, found this hostname in old LockBit 2.0 extortions, linking the “WIN-LIVFRVQFMKO” hostname to another exfiltration endpoint handled by the same provider, Chang Way Technologies Co. Limited.
- In 2021, that hostname appeared in SMTP messages from an M247 LTD Berlin host reported as a “romance scam” in a popular romance and dating scam tracking .
- In March 2022, the hostname appeared in the in a particular conversation dated back to October 2021 where Bentley (one of the group sys admin), was switching a piece of their Tor infrastructure from onion v2 domains to onion v3. In this context, a user named “bloodrush” leaked the hostname by copy-pasting a chat line written by Bentley, and accidentally leaking the hostname.
- Indicators the Threat Intelligence team shared about a June 2023 Ursnif campaign targeting Italy report many remote destinations hosting Ursnif tier 1 command and controls sharing the same hostname (Melbikomas UAB,).
- On August 2023, the security researcher 0xToxin an infection chain leveraging AutoIT scripts to deliver the DarkGate malware, a particular stealer supporting also HVNC and HAnyDesk, and the C2 he decoded was using the same hostname too (XHOST INTERNET SOLUTIONS LP).

This hostname connection is particularly heterogeneous, but it technically makes sense. As specified above, the Windows operating system typically generates a random hostname only during the installation phase, and typical system administration and DevOps practices do not require the Windows installation from scratch so often. Frequently, Sysadmins rely on the so-called Golden Images: snapshots of a pre-installed operating system ready to be customized for the particular application.

So, with a good degree of confidence, we are looking at multiple instances generated from the same base image, likely linked to a single organization, and the extension of this linked infrastructure involves more than 8 thousand hosts worldwide, and at least a third of it is located in CIS countries.

Figure. Potential extension of the related infrastructure
All these pieces draw a very unsettling picture. In fact, since 2019, the hostname has linked a wide range of eCrime activities such as ransomware and data extortions, info-stealing malware spreading, botnet infections, and scams. Basically, seems we are observing a piece of infrastructure linked to a very well-organized criminal gang operating in the full depth of the eCrime ecosystem: stealing initial access credentials, deploying banking bots and ransomware precursors, conducting digital extortions, and laundering money through unaware individuals. And, to make it worse, this hostname seems also related to an ex-Conti sysadmin, dreading a link with the Wizard Spider criminal group.

Unveiling the Criminal Identity

The curious fact of all this investigation is the potential connection with a Russian DevOp professional specialized in managing these machines.

Due to the sensitive nature of this information, we are not going to disclose any details publicly. This TLP:RED information can only be shared with vetted researchers.

Figure. Potential Lockbit Affiliate Public Profile

Conclusion

Our investigation into a recent LockBit incident led us to unwrap the enigmatic mystery of the “golden hostname”, which painted a disturbing portrait of a highly organized criminal enterprise operating deeply into the eCrime ecosystem. The evidence we’ve uncovered points to a single organization using multiple instances likely generated from the same base image.

Since 2019, this hostname has been implicated in a wide array of cybercriminal activities, ranging from ransomware attacks and data exfiltrations to info-stealing malware distribution and scams. Furthermore, the potential link to the ex-Conti sysadmin hints at ties to the notorious Wizard Spider criminal group, raising concerns about the scale and scope of their operations.

In a curious twist, our investigation has led us to a curious overlap between a Russian DevOps professional and the same LockBit incident where we investigated, pointing to a potential connection between this individual and one of the largest cybercriminal enterprises.

This LockBit incident serves as a reminder that shared intelligence and collaboration among cybersecurity professionals are our most potent weapons against the dark forces of the digital world. By piecing together the puzzle of cybercrime, we can better prepare companies and organizations to protect against these modern and extensive threats.

Indicator of Compromise

Potentially Linked Exfiltration Infrastructure:

```
104.206.238.57109.248.11.215135.181.168.29142.202.188.109142.202.189.103142.202.191.18
```