How to target European SMEs with Ransomware? Through Zyxel!

By L M

Published: 2024-11-22 · Archived: 2026-04-05 16:42:20 UTC

Press enter or click to view image in full size

Executive Summary

- The ransomware attack we analyzed was executed in under 1.5 hours, significantly faster than previously reported human-operated attacks, highlights the escalating speed of these threats.
- The threat actor used malware-less lateral movement techniques, leveraging existing system tools like Remote Desktop, coupled with manual credential harvesting and alterations to firewall configurations to accelerate their attack.
- We observed two distinct waves of extortion activity — an earlier wave back in September 2024 using the “unitui57” identifier and a later wave attributed to Helldown activities reported by Sekoia and TrueSec, suggesting evolving tactics or a merging of threat actor operations over time.
- Zyxel’s response to these incidents has been vague, with no clear identification of the vulnerabilities exploited, raising concerns about undisclosed vulnerabilities or a potential supply chain compromise following an August 2024 breach.

Introduction

Recent ransomware attacks are way faster than in the past, especially for SMEs. We recently investigated a case that outshone even the 5-day dwell time for ransomware attacks reported in Mandiant’s M-Trends 2024 and was even faster than the 3-hour cases reported by The DFIR Report (1, 2). The actor we were tracking completed the entire attack kill chain in under 1.5 hours — starting with initial access, progressing through hands-on-keyboard

lateral movement, and culminating in ransomware deployment. Furthermore, we could associate this activity cluster with the recently disclosed Helldown operations discussed within the community.

In this article, we share our findings from an investigation into an emerging ransomware operator active since at least September 2024. Our goal is to provide a clearer understanding of the threats SMEs, which form a crucial part of the broader enterprise supply chain, are currently facing.

Technical Details

Intrusion's TTPs

During our investigation, we uncovered numerous technical details, but here we'll focus on those essential for profiling the threat actor and their malicious toolkit.

First things first, the initial access. We observed the threat actor leveraged direct SSL VPN connections over Zyxel firewalls. This was the starting point of all the actor's activity, which, in the cases we investigate, was able to leverage Active Directory administrative credentials since the first step inside the victim's internal network. But, don't worry, we'll discuss how he could be able to obtain them later because it is a peculiar point that opens many speculations.

Also, the actor conducted lateral movement in a malware-less way, through Remote Desktop (mstsc.exe), nothing new, but extremely effective especially when targeting organizations without advanced user behavioral analytics and lacking advanced detection mechanisms in place. Anyway, in its "living-off-the-land" frenzy, maybe also thanks to the short time frame of the intrusion, the attacker made some mistakes and revealed its own Windows hostname: ALICE43E9.

The actor's internal network discovery phase is pretty trivial but effective. As in many other intrusions, we observed the download and the usage of the Advanced IP Scanner tool, a legit tool by Famatech Corp, in a particular version: 2.5.4594.1, the latest available, built back in 2022.

However, here comes one of the peculiarities of this actor. The crooks also modified the Zyxel configuration by adding a couple of high-priority ACL rules: two ANY ANY rules flattening all the internal network ("Policy-Control_NPF" and "Policy-Control_IPX"). This way, the threat actors were able to speed up the discovery of valuable hosts, such as the ESXi nodes and Veeam backup servers.

The cybercriminals also showed credential harvesting capabilities through the manual analysis of configuration files, for instance, Veeam ones, and extracting them from its encrypted database with tools like "Veeam-Get-Creds.ps1".

Regarding the "action on objective" part of the kill chain, we observed its capability to conduct operations directly on ESXi nodes, running its ransomware payload there to directly encrypt the virtual disk images on the nodes, ending up with this ransom request like this:

Press enter or click to view image in full size

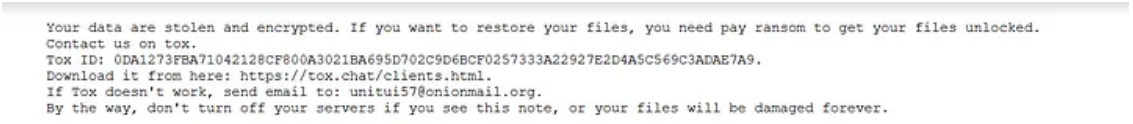

Figure. Example of ransom request

Here we noticed a few more peculiarities. In the meanwhile of their encryption operation, the threat actor was also leveraging a quite peculiar tool to monitor the status of the part of the compromised internal server: “HRSword”. This tool appears to be associated with the open-source “Huorong Sword GUI Frontend” by Beijing Huorong Network Technology Co., Ltd., popular in Chinese-speaking circles.

This tool is also mentioned as part of the kill chain observed in recent Hellcat intrusions by both TrueSec and Sekoia, and this peculiarity gives us another clue the intrusions may be operated by the same threat cluster. Nevertheless, we conducted further investigations, particularly focusing on the malicious artifacts, and uncovered something potentially unique and worth noting.

Malicious Artifacts — Did we miss something?

We decided to dig deeper into the criminal communication channels linked to this intrusion cluster, and that’s when we noticed something interesting.

Specifically, we found evidence of earlier extortion activity in the wild using the same TOX and email extortion channels. These operations, it turns out, began well before the 31 Oct 2024 tweet by @TuringAlex reported by Sekoia, and even before Zyxel’s bulletin on 9 Oct 2024.

Although the Helldown ransomware note started circulating in the wild on November 19, 2024 (hashes: 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19 and cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, as also reported by Sekoia), we observed a different stream of extortion attempts that we were able to trace back to the early days of September 2024, at least the 16th.

Get L M’s stories in your inbox

We identified a series of ransom notes referencing the “unitui57” email account and the TOX ID 0DA1273FBA71042128CF800A3021BA695D702C9D6BCF0257333A22927E2D4A5C569C3ADAE7A9, which differ from those associated with Helldown. Alongside the ransom notes, we uncovered evidence of the Windows encryption tool used during this early wave of attacks.

Press enter or click to view image in full size

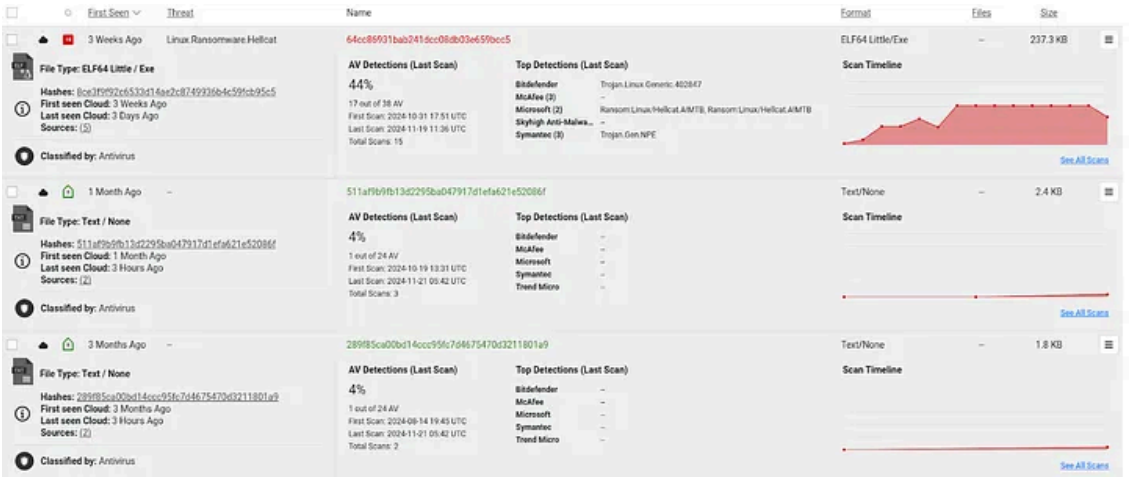

Figure. Samples matching “helldown” (Source:ReversingLabs)

Press enter or click to view image in full size

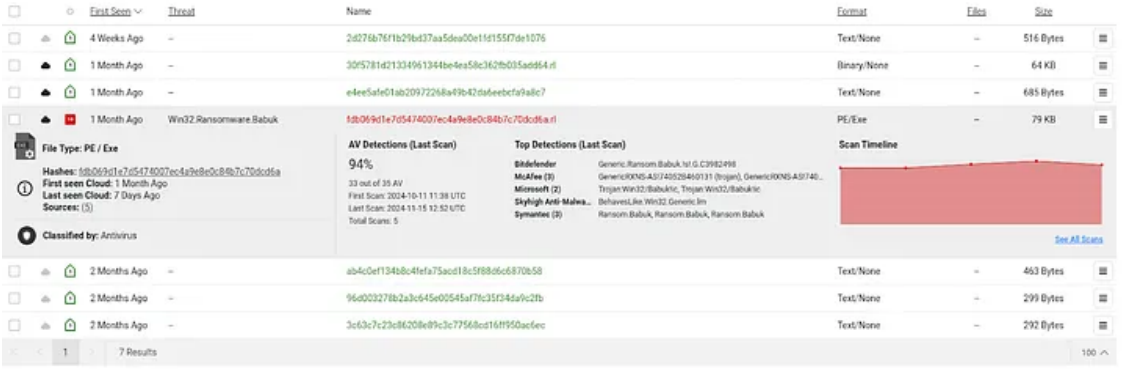

Figure. Samples matching “unitui57” (Source:ReversingLabs)

This Windows sample (hash: fdb069d1e7d5474007ec4a9e8e0c84b7c70dcd6a) matched an old 2023 Astralocker YARA signature from Malpedia by @fxb_b. This is particularly intriguing because Astralocker’s code was based on the old Babuk leaked code, which aligns with the extensive Babuk attributions observed on VT. Interestingly, this Windows locker seems different than the Helldown ones attributed to the later attack waves (hash:b81df159e7e338a3159f27ef3358094f, be37cd010227d7b953b07b93d2e5dadc).

```
win_astralocker_auto pe32_exe_fdb069d1e7d5474007ec4a9e8e0c84b7c70dcd6a.rl
0x61c4:$sequence_0: 8B 55 08 8B 44 0A 04 50 8B 0C 0A 51 E8 8B FD FF FF
0x600a:$sequence_1: 83 C1 02 89 4D FC 83 7D FC 0A 0F 83 DC 00 00 00 8B 55 FC 8B 45 08
0x61ab:$sequence_2: 6B C2 0A 8B 4D 08 33 D2 33 F6 89 14 01
0x61ab:$sequence_3: 6B C2 0A 8B 4D 08 33 D2 33 F6
0x61c7:$sequence_4: 8B 44 0A 04 50 8B 0C 0A 51 E8 8B FD FF FF 83 C4 08 89 45 EC
0x600d:$sequence_5: 89 4D FC 83 7D FC 0A 0F 83 DC 00 00 00 8B 55 FC 8B 45 08 8B 4C D0 04
0x601d:$sequence_6: 8B 45 08 8B 4C D0 04 51 8B 14 D0 52 E8 32 FF FF FF
0x5ff3:$sequence_7: 33 C0 33 F6 89 04 0A 89 74 0A 04
0x61a6:$sequence_8: BA 08 00 00 00 6B C2 0A 8B 4D 08 33 D2 33 F6 89 14 01 89 74 01 04
0x5ff3:$sequence_9: 33 C0 33 F6 89 04 0A 89 74 0A 04 C7 45 FC 00 00 00 00 EB 09
```

Figure. Matching yara sequence on fdb069d1e7d5474007ec4a9e8e0c84b7c70dcd6a

Additionally, even the extortion note from the September wave looks quite different from the November Hellcat ones. The “unitui57” note doesn’t mention the Helldown group or their leak site, while the latter does. However,

despite this discrepancy in the Windows encryption operations, we uncovered some intriguing connections in the ESXi part — so, keep reading the next section.

Press enter or click to view image in full size

Figure. Comparison between Helldown ransom note (left) and the September wave's one (right)

Digging the ESXi Code

We dissected and had the chance to analyze a piece of malware code tied to the previously mentioned September wave, let's call it "unitui57" for short. Notably, the decryption utility from the "unitui57" wave shares the same compiler metadata as the October/November wave, explicitly linked to Helldown.

Figure, september wave ESXi decryptor (3f8aeeec35c6fc2ba8d43c03322a17ce, left), "helldown" wave ESXi encryptor (64cc86931bab241dcc08db03e659bcc5, right)

More interestingly, we noticed that the two samples share a common structure in their encryption/decryption routines, utilizing the Salsa algorithm and implementing compatible intermittent encryption methods.

```
if (__ptr != (undefined8 *)0x0) {
  __offset = 0;
  do {
    lseek64(__fd,__offset,0);
    uVar2 = read(__fd,__buf,__nbytes);
    iVar4 = iVar4 + 1;
    s20_crypt((long)__ptr,1,(undefined *)local_48,0,__buf,(uint)uVar2);
    lseek64(__fd,__offset,0);
    write(__fd,__buf,uVar2 & 0xffffffff);
    __offset = __offset + (long)pcVar5 / lVar3;
  } while (iVar4 < local_7c);
  iVar4 = 1;
  ftruncate64(__fd,(__off64_t)pcVar5);
  close(__fd);
  b_rename(__file);
}
```

```
__ptr = b_gen_salsa_key(0x10);
if (__ptr == (char *)0x0) {
                /* WARNING: Subroutine does not return */
  exit(0);
}
__buf = b_rsa_enc(__ptr,0x10);
__buf_00 = (byte *)b_malloc((ulong)uVar3);
iVar8 = 0;
__offset = 0;
do {
  lseek64(__fd,__offset,0);
  iVar8 = iVar8 + 1;
  uVar6 = read(__fd,__buf_00,(ulong)uVar3);
  s20_crypt((long)__ptr,1,(undefined *)local_48,0,__buf_00,(uint)uVar6);
  lseek64(__fd,__offset,0);
  write(__fd,__buf_00,uVar6 & 0xffffffff);
  __offset = __offset + (long)pcVar1 / lVar7;
} while (iVar8 < iVar2);
lseek64(__fd,0,2);
write(__fd,__buf,0x200);
close(__fd);
b_gen_readme_file(pcVar5);
if (pcVar5 != (char *)0x0) {
  free(pcVar5);
}
```

Figure. Decryption loop ESXi decryptor September wave (left), Encryption loop ESXi encryptor helldown wave (right)

Given this similarity, we believe the ESXi locker used during the early September wave is also likely attributable to the Helldown organization.

The (Very Opaque) Zyxel Response

On 9th October 2023, Zyxel released a security bulletin (link), stating they were tracking “unspecified” threat actors targeting Zyxel devices. The bulletin noted, “In some cases where AD is used and its administrator credentials were also stolen, the hacker uses the SSL VPN connection to access the AD server and encrypt files”.

Aside from a few IoCs — such as the ACL rule names — the clarity stops there. The vendor merely states that these attacks exploited “previous vulnerabilities on earlier firmware versions: ZLD V4.32 to ZLD V5.38”, without referencing any specific CVEs. Instead, simply, they advised users to “upgrade your device to the LATEST firmware (V5.39) if it is still not upgraded”.

Also, on 21 Nov 2024 (link), Zyxel issued another bulletin on the same topic. But, as usual, clarity isn’t their strong suit. This time, they just stated: “We confirm that the reported issues are not reproducible on firmware version 5.39, released on September 3, 2024”.

So, with this little bit of information in hand, we dove into the latest known CVEs associated with Zyxel firewall products, including those highlighted in Zyxel’s 2024–09–03 security bulletin one famously (and indirectly) referenced in the two prior bulletins. But here’s the spoiler: we found no smoking gun, even after analyzing the reserved incident-related data we had at our disposal (*and, if anyone could share info about this, it would be great!*).

Vulnerability	PoC	Exploitability Assessment Related to Ransomware Intrusions
CVE-2023-6397	N/A	Improbable (authenticated DoS)
CVE-2023-6398	N/A	Less likely (authenticated RCE)
CVE-2023-6399	N/A	Improbable (authenticated DoS)
CVE-2023-6764	N/A	Less likely (unauthenticated RCE requiring detailed knowledge of device’s memory layout and configuration)
CVE-2023-48795 (Terrapin)	PoC available	Improbable (SSH MITM)
CVE-2024-3596	PoC available	Less likely (RADIUS request forgery)
CVE-2024-6343	N/A	Improbable (authenticated DoS)
CVE-2024-6387 (regreSSHion)	PoC available	Less likely (unauthenticated RCE requiring a race condition win)
CVE-2024-7203	PoC available	Less likely (authenticated RCE)
CVE-2024-42057	N/A	Less likely (unauthenticated RCE requiring User-Based-PSK authentication mode and a valid user with a username exceeding 28 characters)
CVE-2024-42058	N/A	Improbable (unauthenticated DoS)
CVE-2024-42059	N/A	Less likely (authenticated RCE)
CVE-2024-42060	N/A	Less likely (authenticated RCE)
CVE-2024-42061	N/A	Improbable (reflected XSS)

Anyway, just a couple more interesting tidbits: the community discussion about the 03/09 patch seems to have disappeared, and in August 2024, Zyxel was compromised by Helldown. The criminal gang claimed to have exfiltrated 253 GB of internal documents — possibly including source code?

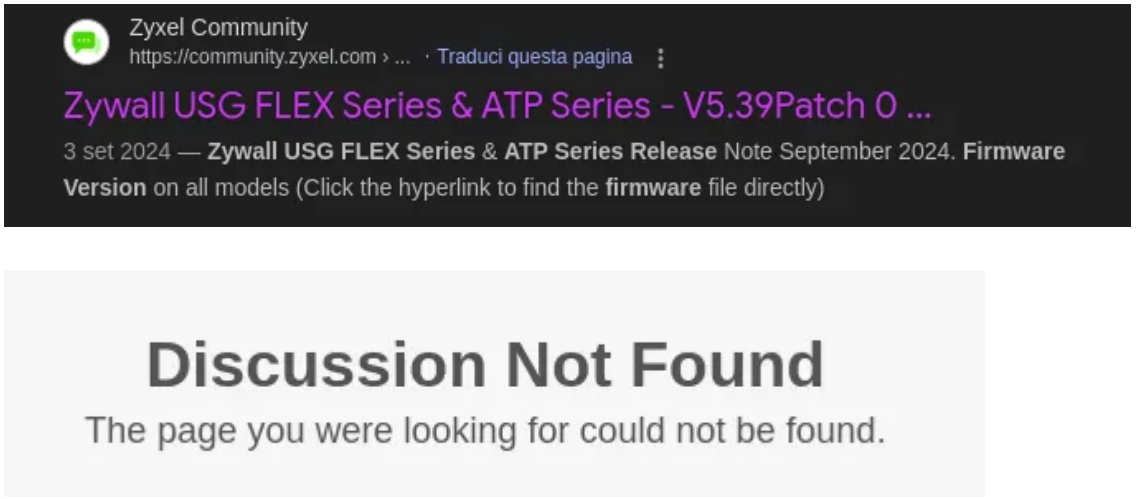

Figure. Sep 3rd, patch community discussion

Press enter or click to view image in full size

Figure. Zyxel compromise claimed in Helldown leak site

Conclusion

The attack chain we investigated aligns with the October/November cases mentioned by Sekoia. Thanks to the evidence we uncovered, we were able to link this campaign to the September wave referenced in the same Sekoia article, which is likely tied to the Zyxel bulletin issued on October 9th.

In the early phase of this campaign, the threat actor appeared to have deliberately concealed their connection to the Helldown group and even used a different locker for Windows environments. This raises several hypotheses about their behavior — perhaps Helldown wanted to distance themselves from these activities, or maybe the initial threat actor joined Helldown a few weeks later. It’s hard to say for certain.

Another unresolved issue is the hypothetical vulnerability exploited by the attacker. Zyxel’s statements remain carefully vague, and our analysis of known exploitable vulnerabilities didn’t uncover any definitive evidence. This leaves room for speculation — ranging from the possibility of an undocumented 0-day to a supply chain compromise linked to the August intrusions. What is clear, however, is that Zyxel’s position remains ambiguous.

Despite their community and security team being involved in these cases from the start, the lack of clarity is puzzling, and the reasons for this remain unclear.

Indicator of Compromise

Extortion channels:

- Tox ID: 0DA1273FBA71042128CF800A3021BA695D702C9D6BCF0257333A22927E2D4A5C569C3ADAE7A9;
- unitui57@onionmail[.org
- Tox ID: 19A549A57160F384CF4E36EE1A24747ED99C623C48EA545F343296FB7092795D00875C94151E
- helldows@onionmail[.org

Threat Actor operator workstation:

- ALICE43E9
