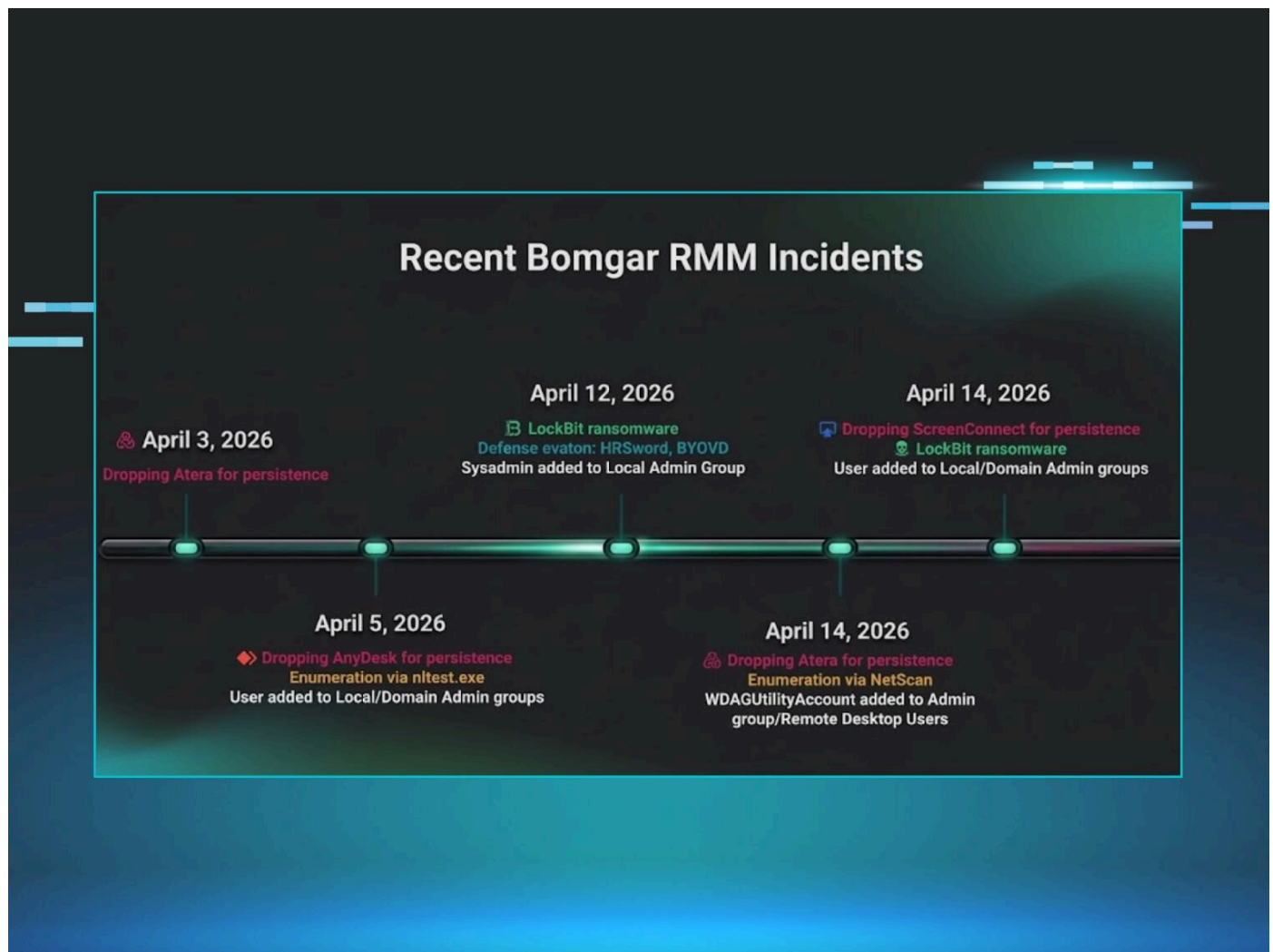


Uptick in Bomgar RMM Exploitation

 huntress.com/blog/uptick-bomgar-exploitation



Acknowledgments: Special thanks to Olly Maxwell, Josh Kiriakoff, Jordan Sexton, Ryan Dowd, Jamie Dumas, Amelia Casley, Austin Worline, and Lindsey O'Donnell-Welch for their contributions to this research and blog.

Over the past two weeks, the Huntress Security Operations Center (SOC) has seen an uptick in incidents involving compromised Bomgar remote monitoring and management (RMM) instances. The uptick follows intermittent waves of exploitation we have seen over the past two months, after BeyondTrust first disclosed a critical-severity flaw (CVE-2026-1731) in Bomgar in February.

On February 6, 2026, BeyondTrust issued fixes for [the flaw](#) in Bomgar (rebranded as BeyondTrust Remote Support), which could be exploited by an unauthenticated attacker to remotely execute code. During this timeframe, the SOC observed an initial spike in exploitation of Bomgar RMMs

starting on February 12, which involved at least 10 impacted organizations. Then, starting around April 3, the SOC saw another increase in attacks.

Currently, we do not have further insight into the specific root cause behind these attacks, but the incidents likely stem from the exploitation of CVE-2026-1731. We see malicious processes stemming from bomgar-scc.exe, and we can see that the impacted organizations are running versions of Bomgar that are outdated.

Key takeaways

- Huntress has seen multiple incidents involving Bomgar RMM since April 3, 2026. One of those incidents on April 14 involved ransomware deployed from the Bomgar RMM instance at a dental software company, which impacted three downstream companies. Another incident on April 15 on a Managed Service Provider (MSP) led to the mass isolation of 78 businesses, and we observed subsequent exploitation across four downstream customers.
- In some incidents, threat actors have used the compromised Bomgar instances to deploy the LockBit ransomware. Based on several clues, the threat actors behind the attacks are suspected to be using the previously leaked LockBit 3.0 builder.
- Threat actors have also used their access via Bomgar to conduct domain reconnaissance, perform network enumeration via NetScan, add Administrator users for persistence, and execute further RMMs like AnyDesk and Atera.
- This most recent uptick in Bomgar-related incidents follows an initial wave of attacks observed by the SOC in February, when CVE-2026-1731 was first disclosed.



Figure 1: Detection timeline showing malicious processes stemming from bomgar-scc.exe

The tradecraft

Targeting downstream customers

In several incidents, threat actors used compromised Bomgar RMMs belonging to organizations in order to target their downstream customer base. On April 15, Huntress observed a serious compromise involving an MSP Bomgar account with high privileges that was used to deploy remote access tools onto a domain controller. By targeting an MSP, the attackers were able to establish persistence on downstream client environments managed by the MSP.

The actor moved quickly to conduct account reconnaissance, create a new local account, and elevate it first into the Local Administrators Group and then into Domain Admins—effectively creating a persistent backdoor with domain-wide control. The intrusion did not stop at privilege escalation. With administrative control in place, the actor deployed additional remote access tools including AnyDesk (C:\Users\support\Documents\AnyDesk.exe).

LockBit ransomware deployment

SOC analysts saw multiple incidents that resulted in the deployment of LockBit ransomware, and observed several similarities across the incidents.

In another incident that was first detected on April 14, a ransomware campaign hit multiple organizations through a compromised Bomgar remote support environment. The compromised RMM instance belonged to a dental software company with software installed across dozens of organizations. Here are some of the tactics we saw threat actors taking after accessing victim environments:

- Adding credentials for a user (Adminpwd123.1) and then adding the user to the Local Administrators Group and Domain Administrative Group (net localgroup administrators [REDACTED] /add and net group "domain admins" [REDACTED] /add) as a persistence mechanism.
- Utilizing a ScreenConnect remote access client as an additional persistence mechanism in the targeted environment (which was seen with C:\Program Files (x86)\ScreenConnect Client (0a42c9161c039ecc)\)
- Executing LB3.exe from the user's Desktop via a command prompt session and targeting multiple directories (including local drives and the Microsoft SQL Server installation path).

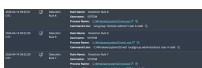


Figure 2: Timeline of threat actor activity before executing LB3.exe

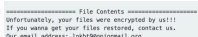
In a separate incident on April 12, SOC analysts observed a rogue Bomgar RMM instance being used to gain access to endpoints, which resulted in successful ransomware execution on the network. Here, we also saw threat actors use the rogue RMM instance to create and add a new user to the Local Administrators Group.

However, in this incident, threat actors also aimed to kill security tooling by deployed suspicious drivers, seen in the binary paths C:\Windows\System32\drivers\hrwfpdrv.sys and C:\temp\PoisonX.sys. The latter (PoisonX.sys) may be linked to PoisonKiller, a Bring Your Own Vulnerable Driver (BYOVD) tool designed to terminate EDR agents (the tool was likely [listed on GitHub](#) at the beginning of April, but has since been removed).

The SOC also observed the actor using HRSword.exe, which is legitimate software abused by cybercriminals to bypass security defenses.

Finally, the threat actor executed the ransomware binary through the Bomgar RMM session, resulting in the successful encryption of the endpoint via (again) the executable LB3.exe.

One noteworthy aspect of this incident was that the ransom note dropped during the attack did not match the “style” of LockBit ransomware attacks we have seen in the past. The SOC saw a similarly styled ransom note dropped in an April 9 incident, where the Huntress agent was added to the targeted endpoint mid-compromise, and both ransom notes shared the same email (lokbt9@onionmail[.]org). There are several potential reasons why the style of the ransom note appears to be different, but one possibility is that the threat group behind this incident was using the LockBit builder that had previously been leaked in 2022.



===== File Contents =====
Unfortunately, your files were encrypted by us!!!
If you want get your files restored, contact us.
Our email address: lokbt9@onionmail.org.

Figure 3: An excerpt from the ransom note

Other TTPs

We observed several other tactics across attacks involving Bomgar RMMs. In another incident seen on April 14, threat actors used their access via a compromised Bomgar instance to add a built-in account (WDAGUtilityAccount) to the Administrator Group and Remote Desktop Users, before setting the credentials for the account to 123123qwEqwE (a password that’s been seen in previous incidents). This account then executed the AnyDesk remote desktop application and executed NetScan, a network enumeration tool.

We also saw threat actors using their existing access via the Bomgar RMM to deploy additional RMMs for further persistence, something [we’ve seen frequently in the past](#). During an April 5 incident, the threat actors first performed domain reconnaissance (via nltest.exe) and then

installed a new user account and added it to the local Administrators group and Domain Admins group. Finally, they installed AnyDesk as seen in the following command line: anydesk.exe --install "C:\Program Files (x86)\AnyDesk"

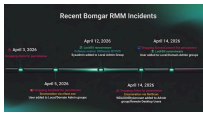


Figure 4: A comparison of some of the recent incidents involving Bomgar the SOC has seen

In an April 3 incident, the SOC saw threat actors use a Bomgar remote access session to execute commands through the Bomgar remote shell interface with SYSTEM privileges. These included launching Windows Installer (msiexec.exe) in the PerfLogs directory (C:\Windows\System32\msiexec.exe /i C:\PerfLogs\setup.msi). The setup.msi was an installer for the Atera remote management tool. Separately, a scheduled task was created (AteraAgentServiceWatchdog).

The Bomgar client (which was signed by Bomgar Corporation) was an outdated version vulnerable to CVE-2026-1731 (version 21.1.3). These clues led the SOC to suspect that the attackers in this particular incident were exploiting Bomgar’s existing vulnerability, which has been patched since February in version 25.3.2 of Bomgar/Remote Support (versions 25.3.1 and prior are impacted) and version 25.1 of Privileged Remote Access (versions 24.3.4 and prior are impacted).

Bomgar/Remote Support	
Version	21.1.3
Product	Remote Support
Product Version	21.1.3

Figure 5: Fixed versions of Bomgar RMM

Many of these TTPs were seen during previous incidents since the initial disclosure of CVE-2026-1731. During the course of a retrospective threat hunt, we also observed an incident likely to have started March 11 stemming from suspicious Bomgar activity. Here, a renamed SimpleHelp RMM was dropped onto the system, which was executed out of the PerfLogs directory (c:\PerfLogs\InputUpdate.exe) and configured to the IP address 146.70.41[.]131.

Ongoing incidents

We wanted to highlight this recent uptick in exploitation of this specific RMM, leading to the access of partner environments. Here are a few ways that businesses can protect themselves, particularly if they already have Bomgar in their environments:

- Make sure that you have applied the patches for CVE-2026-1731 (check out BeyondTrust’s security advisory [for more information](#))

- Monitor environments for suspicious users added to the Local Administrators/Domain Administrators groups
- Audit RMMs in order to track ones that are currently used or authorized. Check curated lists like LOLRMM to better understand what RMM tools could potentially be abused by threat actors
- Check logs for instances where RMMs were executed to find suspicious RMMs
- Check the versions that your Bomgar/Remote Support or Privileged Remote Access device is running by logging into the /appliance admin interface and viewing the software version on the status page.

Indicators of Compromise

Indicator	Description
LB3.exe SHA256: 538b3b36dd8a30e721cc8dc579098e984cf8ed30b71d55303db45c7344f7a4cf	Ransomware executable in April 12 incident
LB3.exe SHA256: 3529b1422da886b7d04555340dfb1efd44a625c2921af6df39819397176956d6	Ransomware executable in April 14 incident
Adminpwd123.1	Password used by attacker in April 14 incident
123123qwEqwE	Password used by attacker in April 14 incident

InputUpdate.exe	Renamed SimpleHelp RMM on March 11
SHA256: bc9635dcc3444c18b447883c6bc1931e5373e48c7dbfaa607285a9fb668b03ea	
146.70.41[.]131	IP address configured to March 11 SimpleHelp RMM
lokbt9@onionmail[.]org	Email on ransom note in April 12 incident
HRSword.exe	HRSword tool used by threat actors in April 12 incident
SHA256: b44dd12179a15a7d89c18444d36e8d70b51d30c7989d3ab71330061401f731fe	
PoisonX.sys	Driver used by threat actor in April 12 incident
SHA256: a5035cbd6c31616288aa66d98e5a25441ee38651fb5f330676319f921bb816a4	
hrwfpdrv.sys	Driver used by threat actor in April 12 incident