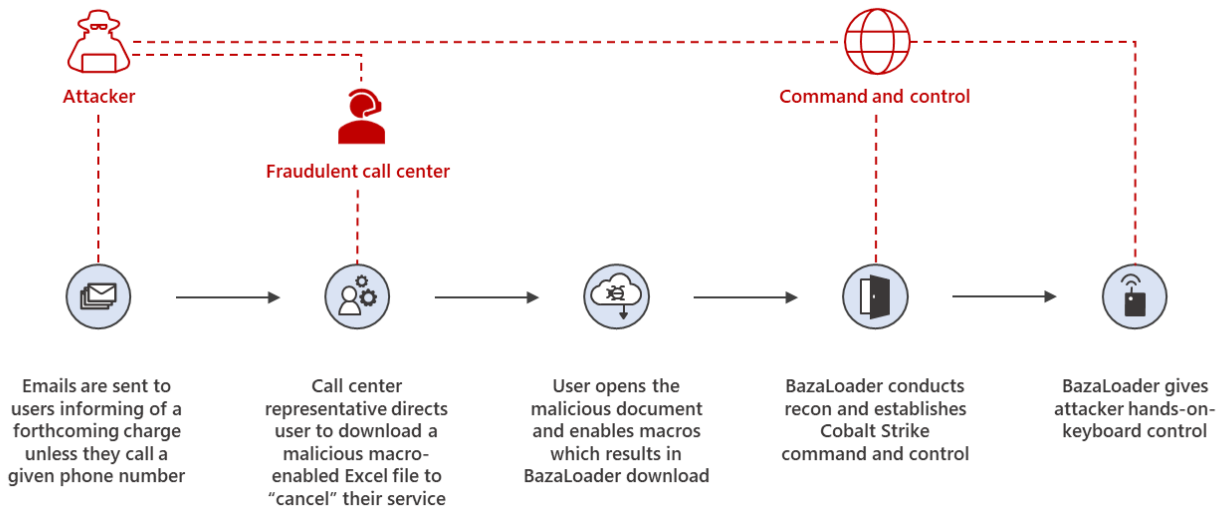
BazaCall: Phony call centers lead to exfiltration and ransomware

microsoft.com/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/

July 29, 2021



Our continued investigation into BazaCall campaigns, those that use fraudulent call centers that trick unsuspecting users into downloading the BazaLoader malware, shows that this threat is more dangerous than what's been discussed publicly in other security blogs and covered by the media. Apart from having backdoor capabilities, the BazaLoader payload from these campaigns also gives a remote attacker hands-on-keyboard control on an affected user's device, which allows for a fast network compromise. In our observation, attacks emanating from the BazaCall threat could move quickly within a network, conduct extensive data exfiltration and credential theft, and distribute ransomware within 48 hours of the initial compromise.

Additional resources
Protect your organization against ransomware: aka.ms/ransomware

Learn how attackers operate: Human-operated ransomware attacks: A preventable disaster

BazaCall campaigns forgo malicious links or attachments in email messages in favor of phone numbers that recipients are misled into calling. It's a technique reminiscent of vishing and tech support scams where potential victims are being cold-called by the attacker, except in BazaCall's case, targeted users *must* dial the number. And when they do, the users are

connected with *actual* humans on the other end of the line, who then provide step-by-step instructions for installing malware into their devices. Thus, BazaCall campaigns require direct phone communication with a human and social engineering tactics to succeed. Moreover, the lack of obvious malicious elements in the delivery methods could render typical ways of detecting spam and phishing emails ineffective.

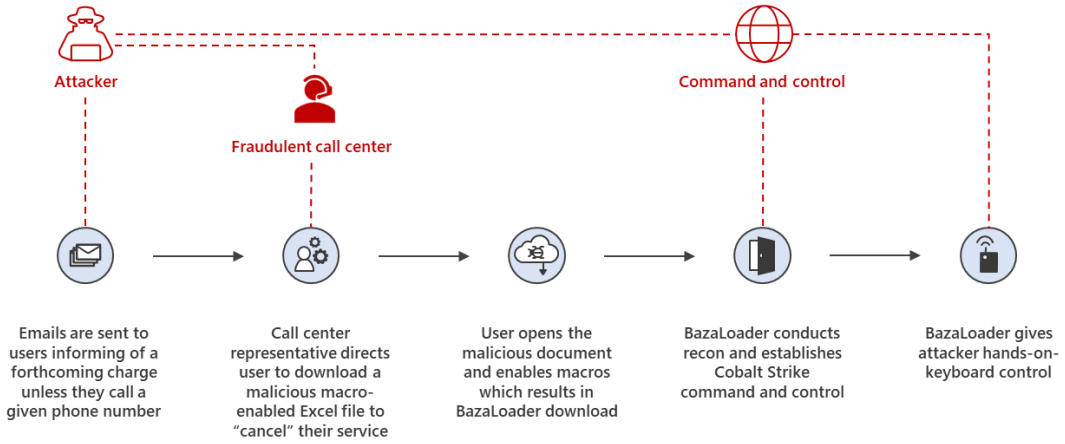


Figure 1. The flow of a typical BazaCall attack, from the spam email to social engineering to the payload being downloaded and hands-on-keyboard attacks

The use of another human element in BazaCall's attack chain through the abovementioned hands-on-keyboard control further makes this threat more dangerous and more evasive than traditional, automated malware attacks. BazaCall campaigns highlight the importance of cross-domain optics and the ability to correlate events in building a comprehensive defense against complex threats.

Microsoft 365 Defender orchestrates protection across domains to deliver coordinated defense. In the case of BazaCall, Microsoft Defender for Endpoint detects malware and attacker behavior resulting from the campaign, and these signals inform Microsoft Defender for Office 365 protections against related emails, even if these emails don't have the typical malicious artifacts. Microsoft threat analysts who constantly monitor BazaCall campaigns enrich the intelligence on this threat and enhance our ability to protect customers.

In this blog post, we discuss how a recent BazaCall campaign attempts to compromise systems and networks through the mentioned human elements and how Microsoft defends against it.

Out with the links and attachments, in with the customer service phone numbers

BazaCall campaigns begin with an email that uses various social engineering lures to trick target recipients into calling a phone number. For example, the email informs users about a supposed expiring trial subscription and that their credit card will soon be automatically charged for the subscription's premium version. Each wave of emails in the campaign uses a different "theme" of subscription that is supposed to be expiring, such as a photo editing service or a cooking and recipes website membership. In a more recent campaign, the email does away with the subscription trial angle and instead poses as a confirmation receipt for a purchased software license.

Unlike typical spam and phishing emails, BazaCall's do not have a link or attachment in its message body that users must click or open. Instead, it instructs users to call a phone number in case they have questions or concerns. This lack of typical malicious elements—links or attachments—adds a level of difficulty in detecting and hunting for these emails. In addition, the messaging of the email's content might also add an air of legitimacy if the user has been narrowly trained to avoid typical phishing and malware emails but not taught to be wary of social engineering techniques.

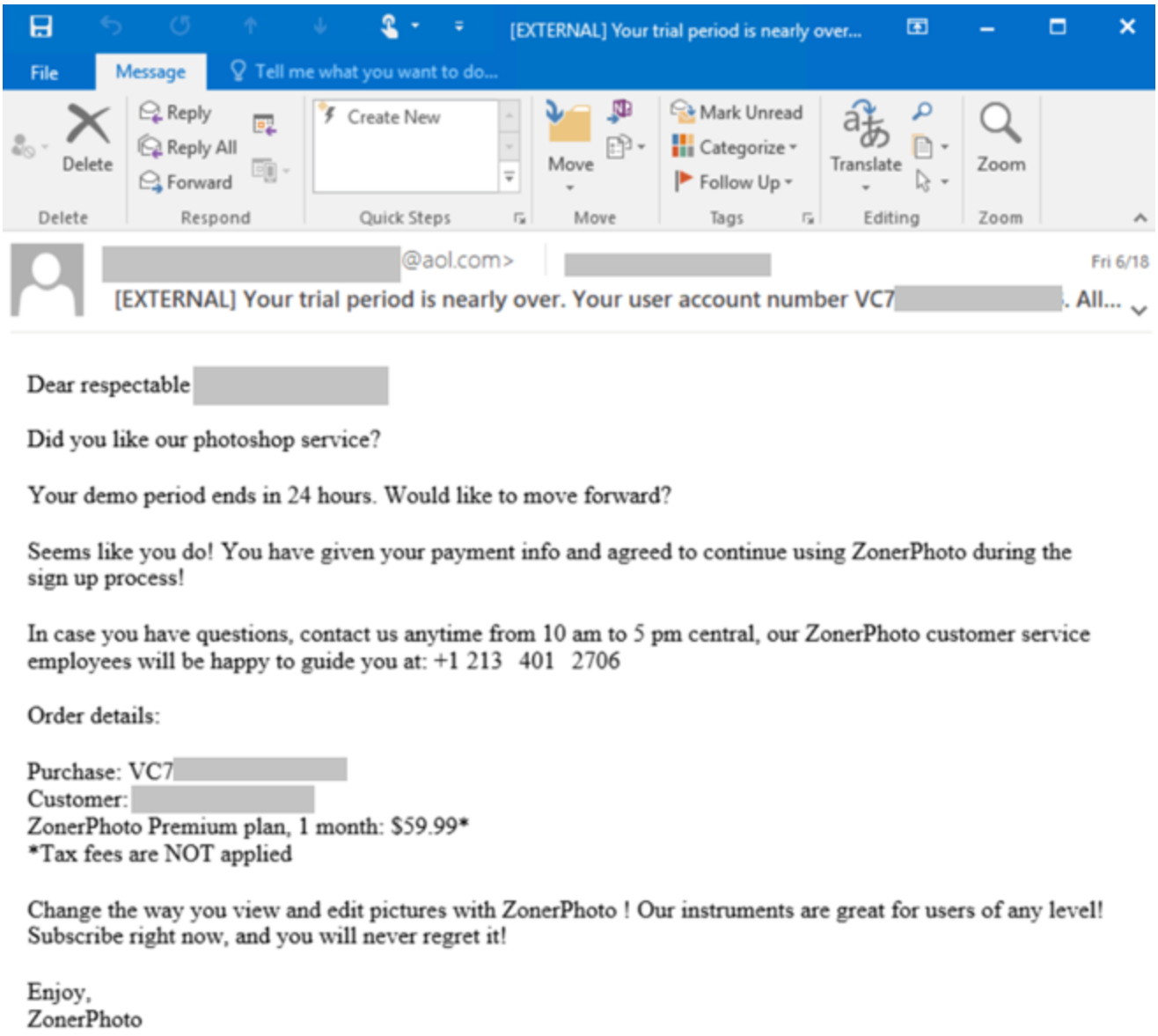


Figure 2. A typical BazaCall email, claiming that the user's trial for a photo editing service will soon expire, and that they will be automatically charged. A fake customer service number is provided to help cancel the subscription.

Each BazaCall email is sent from a different sender, typically using free email services and likely-compromised email addresses. The lures within the email use fake business names that are similar to the names of real businesses. A recipient who then searches the business name online to check the email's legitimacy may be led to believe that such a company exists and that the message they received has merit.

Some sample subject lines are listed below. They each have a unique "account number" created by the attackers to identify the recipients:

- Soon you'll be moved to the Premium membership, as the demo period is ending. Personal ID: KT[unique ID number]

- Automated premium membership renewal notice GW[unique ID number] 👴
- Your demo stage is nearly ended. Your user account number VC[unique ID number]. All set to continue?
- Notification of an abandoned road accident site! Must to get hold of a manager! [body of email contains unique ID number]
- Thanks for deciding to become a member of BooyaFitness. Fitness program was never simpler before [body of email contains unique ID number]
- Your subscription will be changed to the gold membership, as the trial is ending. Order: KT[unique ID number]
- Your free period is almost ended. Your member's account number VC[unique ID number]. Ready to move forward?
- Thank you for getting WinRAR pro plan. Your order # is WR[unique ID number].
- Many thanks for choosing WinRAR. You need to check out the information about your licenses [body of email contains unique ID number]

While the subject lines in most of the observed campaigns contain similar keywords and occasional emojis, each one is unique because it includes an alphanumeric sequence specific to the recipient. This sequence is always presented as a user ID or transaction code, but it actually serves as a way for the attacker to identify the recipient and track the latter's responses to the campaign. The unique ID numbers largely follow the same pattern, which the regular expression *[A-Z]{1,3}(?:\d{9,15})* can surface, for example, *L0123456789* and *KT01234567891.*

In one recent BazaCall campaign, the unique ID was present in the body of the email, but not in the subject line:

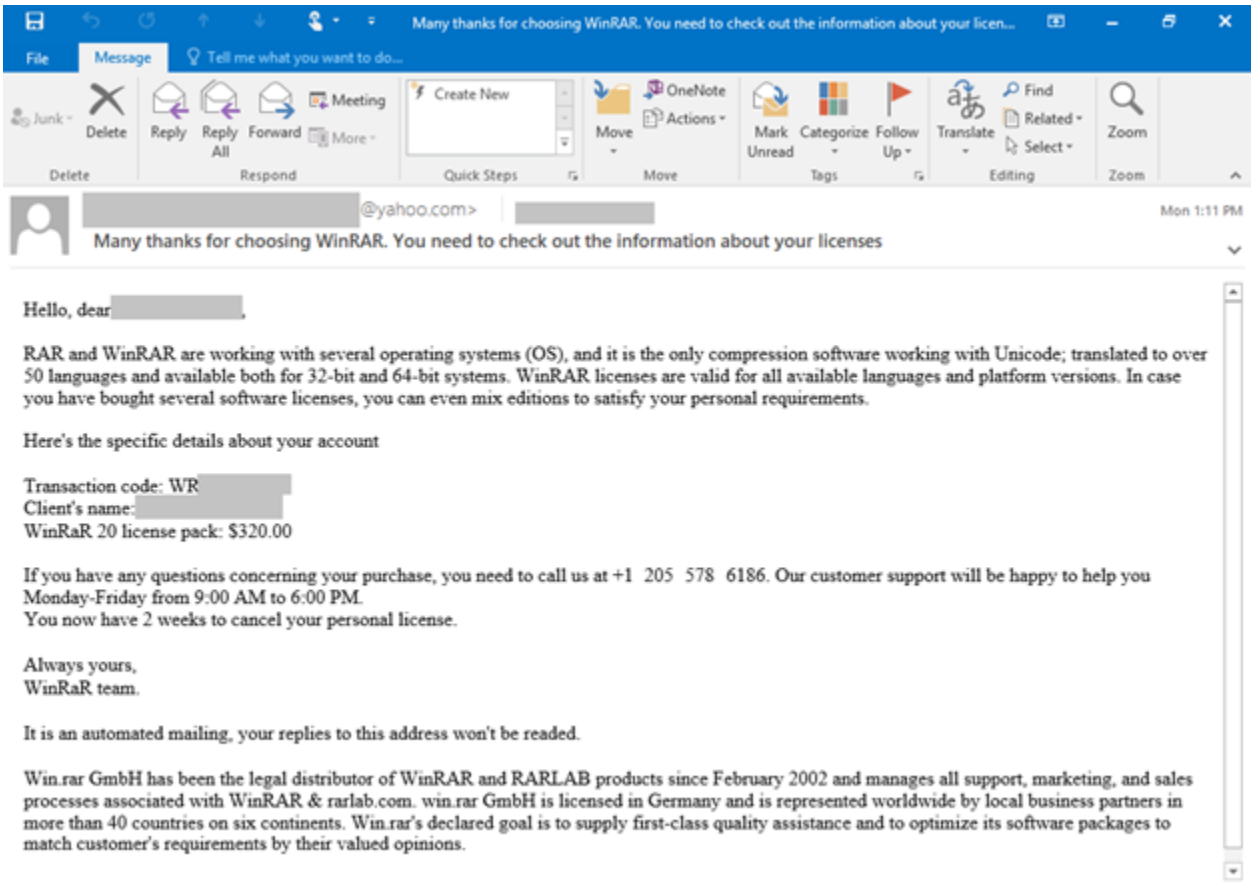


Figure 3. A recent BazaCall email with the unique ID present only in the message body.

If a target recipient does decide to call the phone number indicated in the email, they will speak with a real person from a fraudulent call center set up by BazaCall's operators. The call center agent serves as a conduit to the next phase of the attack: during their conversation, an agent tells the caller they can help cancel the supposed subscription or transaction. To do so, the agent asks the caller to visit a website.

These websites are designed to look like legitimate businesses, some of which even impersonate actual companies. However, we have noted that some domain names do not always match the name of the fictitious business included in the email. For example, an email claiming that a user's free trial for "Pre Pear Cooking" was set to expire was paired with the domain, "topcooks[.]us".

Figure 4. A sample website used in the BazaCall campaign. It mimics a real recipe website but is attacker-controlled.

The call center agent then instructs the user to navigate to the account page and download a file to cancel their subscription. The file is a macro-enabled Excel document, with names such as “cancel_sub_[unique ID number].xlsb.” Note that in some instances, we observed that even if security filters such as Microsoft Defender SmartScreen are enabled, users intentionally bypass it to download the file, which indicates that the call center agent is likely instructing the user to circumvent security protocols, with the threat that their credit cards will be charged if they don’t. Again, this demonstrates the effectiveness of social engineering tactics used in BazaCall attacks.

The downloaded Excel file displays a fake notification that it is protected by Microsoft Office. The call center agent then instructs the user to click on the button that enables editing and content (macros) to view the spreadsheet’s contents. If the user enables the macro, BazaLoader malware is delivered to the device.

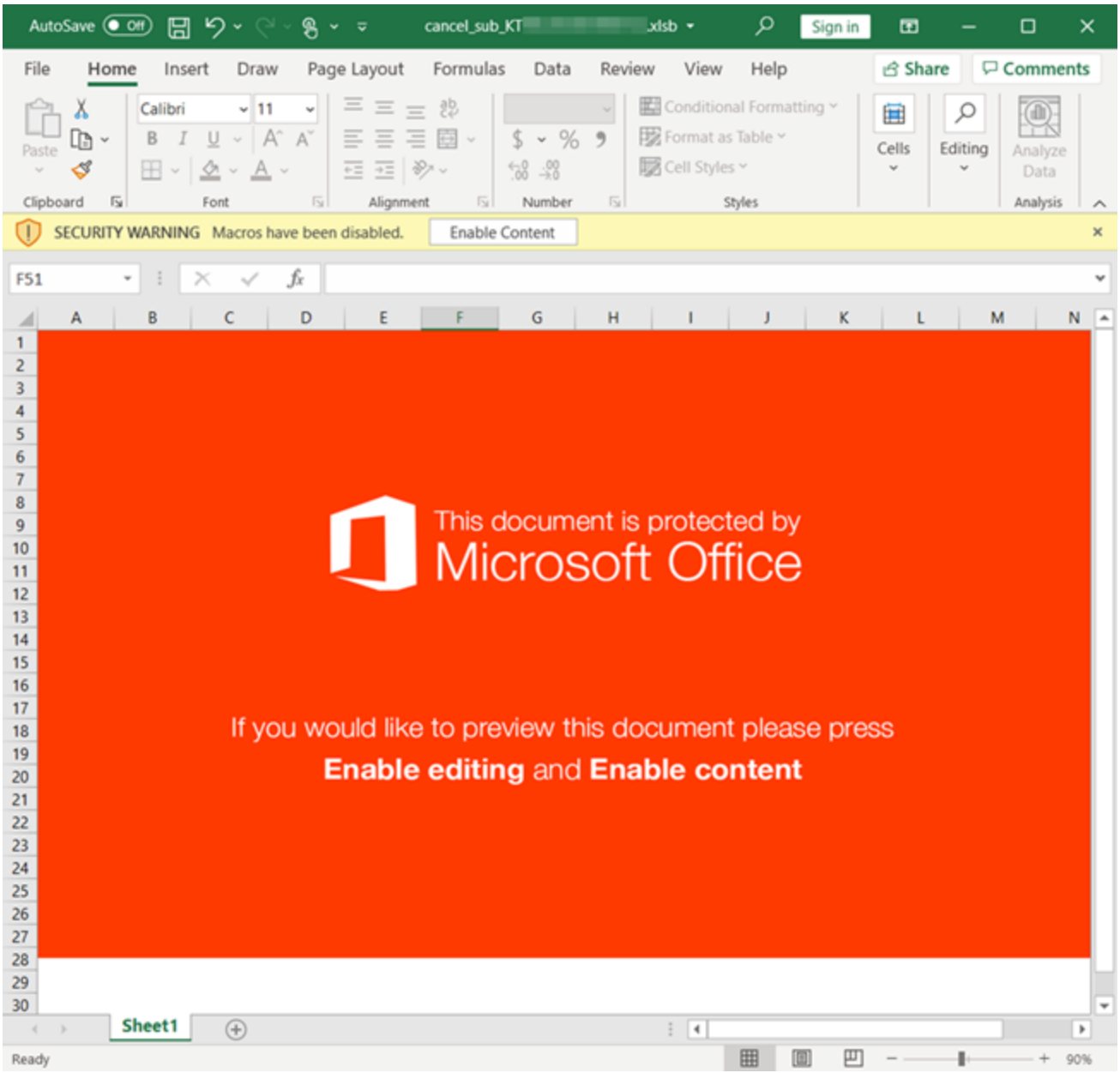


Figure 5. An Excel document used by the attackers, prompting the user to enable malicious code.

Hands-on-keyboard control for selective data exfiltration

The enabled macro on the Excel document creates a new folder named with a random string of characters in the *%programdata%* folder. It then copies *certutil.exe*, a known living-off-the-land binary (LOLBin), from the *System* folder and places the copy of *certutil.exe* into the newly created folder as a means of defense evasion. Finally, the copy of *certutil.exe* is renamed to match the random string of characters in the folder name.

The macro then uses the newly renamed copy of *certutil.exe* to connect to the attacker infrastructure and download BazaLoader. This downloaded payload is a malicious dynamic link library (*.dll*) and is loaded by *rundll32.exe*. *Rundll32* then injects a legitimate *MsEdge.exe*

process to connect to a BazaLoader command-and-control (C2) and establish persistence by using Edge to create a *.lnk* (shortcut) file to the payload in the *Startup* folder. The injected *MsEdge.exe* is also used for reconnaissance, collecting system and user information, domains on the networks, and domain trusts.

The *rundll32.exe* process retrieves a Cobalt Strike beacon that enables the attacker to have hands-on-keyboard control of the device. Now with direct access, the attacker performs reconnaissance on the network and searches for local administrators and high-privilege domain administrator account information.

The attacker also conducts further extensive reconnaissance using ADFind, a free command-line tool designed for Active Directory discovery. Often, information gathered from this reconnaissance is saved to a text file and viewed by the attacker using the *"Type"* command in the command prompt.

Once the attacker has established a list of target devices on the network, they use Cobalt Strike's custom, built-in PsExec functionality to move laterally to the targets. Each device the attacker lands on establishes a connection to the Cobalt Strike C2 server. Additionally, certain devices are used for additional reconnaissance by downloading open-source tools designed to steal browser passwords. In some instances, the attackers also used WMIC to move laterally to high-value targets, such as Domain Controllers.

When the attacker lands on a selected high-value target, they use 7-Zip to archive intellectual property for exfiltration. The archived files are named after the type of data they contain, such as IT information, or information about security operations, finance and budgeting, and details specific to each target's industry. The attacker then uses a renamed version of the open-source tool, *RClone,* to exfiltrate these archives to an attacker-controlled domain.

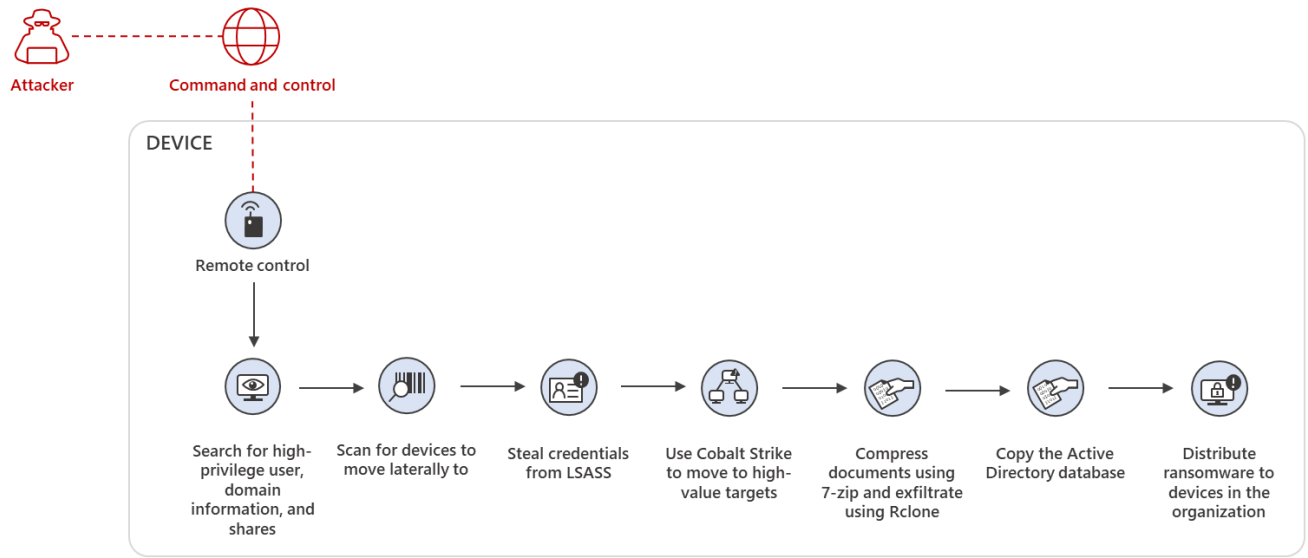


Figure 6 Post-compromise activity on the target, including exfiltration and ransomware.

Finally, on domain controller devices, the attacker uses *NTDSUtil.exe*—a legitimate tool typically used to create and maintain the Active Directory database—to create a copy of the *NTDS.dit* Active Directory database, in either the *%programdata%* or *%temp%* folders, for subsequent exfiltration. NTDS.dit contains user information and password hashes for all users in the domain.

In some instances, data exfiltration appeared to be the primary objective of the attack, which would typically be in preparation for future activity. However, in other instances, the attacker deploys ransomware after conducting the previously described activity. In those cases where ransomware was dropped, the attacker used high-privilege compromised accounts in conjunction with Cobalt Strike's PsExec functionality to drop a Ryuk or Conti ransomware payload onto network devices.

Detecting BazaCall through cross-domain visibility and threat intelligence

While many cybersecurity threats rely on automated, drive-by tactics (for example, exploiting system vulnerabilities to drop malware or compromising legitimate websites for a watering hole attack) or develop advanced detection evasion methods, attackers continue to find success in social engineering and human interaction in attacks. The BazaCall campaign replaces links and attachments with phone numbers in the emails it sends out, posing challenges in detection, especially by traditional antispam and anti-phishing solutions that check for those malicious indicators.

The lack of typical malicious elements in BazaCall's emails and the speed with which their operators can conduct an attack exemplify the increasingly complex and evasive threats that organizations face today. Microsoft 365 Defender provides the cross-domain visibility and coordinated defense to protect customers against such threats. The ability to correlate events across endpoints and emails is crucial in the case of BazaCall, given its distinct characteristics. Microsoft Defender for Endpoint detects implants such as BazaLoader and Cobalt Strike, payloads such as Conti and Ryuk, and subsequent attacker behavior. These endpoint signals are correlated with email threat data, informing Microsoft Defender for Office 365 to block the BazaCall emails, even if these emails don't have the typical malicious artifacts.

Microsoft 365 Defender further enables organizations to defend against this threat through rich investigations tools like advanced hunting, allowing security teams to locate related or similar activities and seamlessly resolve them.

Justin Carroll *and* ***Emily Hacker***

Microsoft 365 Defender Threat Intelligence Team

Advanced hunting queries

The following Advanced Hunting Queries are accurate as of the time of publish of this blog. For the most up-to-date queries, please visit aka.ms/BazaCall.

To locate possible exploitation activity, run the following queries in the Microsoft 365 Defender portal.

BazaCall emails

To look for malicious emails matching the patterns of the BazaCall campaign, run this query.

```
EmailEvents
| where Subject matches regex @"[A-Z]{1,3}\d{9,15}"
and Subject has_any('trial', 'free', 'demo', 'membership', 'premium',
'gold',
'notification', 'notice', 'claim', 'order', 'license', 'licenses')
```

BazaCall Excel file delivery

To look for signs of web file delivery behavior matching the patterns of the BazaCall campaign, run this query.

```
DeviceFileEvents
| where FileOriginUrl has "/cancel.php" and FileOriginReferrerUrl has
"/account"
or FileOriginUrl has "/download.php" and FileOriginReferrerUrl has "/case"
```

BazaCall Excel file execution

To surface the execution of malicious Excel files associated with BazaCall, run this query.

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "excel.exe"
and ProcessCommandLine has_all('mkdir', '&& copy', 'certutil.exe')
```

BazaCall Excel file download domain pattern

To look for malicious Excel files downloaded from *.XYZ* domains, run this query.

```
DeviceNetworkEvents
| where RemoteUrl matches regex @".{14}\.xyz/config\.php"
```

BazaCall dropping payload via certutil

To look for the copy of *certutil.exe* that was used to download the BazaLoader payload, run this query.

```
DeviceFileEvents
| where InitiatingProcessFileName !~ "certutil.exe"
| where InitiatingProcessFileName !~ "cmd.exe"
| where InitiatingProcessCommandLine has_all("-urlcache", "split", "http")
```

NTDS theft

To look for theft of Active Directory in paths used by this threat, run this query.

```
DeviceProcessEvents
| where FileName =~ "ntdsutil.exe"
| where ProcessCommandLine has_any("full", "fu")
| where ProcessCommandLine has_any ("temp", "perflogs", "programdata")
// Exclusion
| where ProcessCommandLine !contains @"Backup"
```

Renamed Rclone data exfiltration

To look for data exfiltration using renamed Rclone, run this query.

```
DeviceProcessEvents
| where ProcessVersionInfoProductName has "rclone" and not(FileName has
"rclone")
```

RunDLL Suspicious Network Connections

To look for RunDLL making suspicious network connections, run this query.

```
DeviceNetworkEvents
| where InitiatingProcessFileName =~ 'rundll32.exe' and
InitiatingProcessCommandLine has ",GlobalOut"
```

Learn how your organization can stop attacks through automated, cross-domain security and built-in AI with Microsoft Defender 365.