ReliaQuest Uncovers New Black Basta Social Engineering Technique

By ReliaQuest Threat Research Team 25 October 2024

Published: 2024-10-25 · Archived: 2026-04-05 13:29:09 UTC

Updated December 12, 2024

In late November 2024, ReliaQuest responded to several incidents related to Black Basta activity that resulted in the identification of new TTPs. Initially, users were targeted by a flood of emails—with one user receiving as many as 326—in activity that was reminiscent of previous Black Basta activity. Following these emails, additional alerts were raised for the same user, regarding suspicious Microsoft Teams communications that were originating from Russia. The domain linked to the suspicious Microsoft Teams messages were unusual, as they belonged to a legitimate organization. This deviation indicated that this organization had been compromised by the Black Basta group, which used its domain to target additional organizations.

The compromised tenant in this instance followed the same naming convention as previously identified malicious tenants used in Black Basta activity. Previously, tenants displayed “Help Desk” or “Support Team” as their username. In the new incident, the UserId was “technicalsupport,” which also inherited the display name “Help Desk.”

Shortly after the user received the Microsoft Teams message, the threat actor initiated a call attempting to manipulate the end user into downloading “filter_update.vbs”. The execution of this script resulted in commands attempting to enumerate the organization’s domain, create a network connection to IP address 179.60.149[.]194, and download 3 files: “file.zip”, “script.a3x”, and “Autoit3.exe”. These files resulted in ReliaQuest detections firing for file downloads via PowerShell, PowerShell Obfuscated Script and Emergency IoCs. Execution of the additional files failed, and as a result the threat was contained.

Detection Opportunities

Remain vigilant for the following Microsoft Teams activity, which is likely to be malicious.

- Microsoft Teams communications originating from Russia, where the UserId or Display Name includes keywords like “Help Desk” or “Support Team.”
- Where the UserID’s domain is not included on allow lists.
- Microsoft Teams communication where the event type is MessageSent, the UserId contains “onmicrosoft.com,” and where there are multiple recipients within a short time.
- Microsoft Teams communication where the event type is MessageCreatedHasLink, UserId contains “onmicrosoft.com,” or sourcing from Russia in which the MessageURL contains “sharepoint.com.”

- Microsoft Teams messages where the MessageURL does not contain your organization's Sharepoint details.

IoCs

1helpyou.onmicrosoft[.]com

Assistingyou.onmicrosoft[.]com

Spamshieldmanager.onmicrosoft[.]com

SecurityFusion.onmicrosoft[.]com

Brandonsupport.onmicrosoft[.]com

Supporthelper.onmicrosoft[.]com

Servicedeskadmin.onmicrosoft[.]com

Radolud.onmicrosoft[.]com

Hegss.onmicrosoft[.]com

Asparren.onmicrosoft[.]com

Freeuk566.onmicrosoft[.]com

Bbacons.onmicrosoft[.]com

Dbvy.onmicrosoft[.]com

Editor's note: The following was first published on October 25, 2024.

What Happened?

In October 2024, ReliaQuest responded to an alert for Impacket activity. During the investigation, we discovered a wider trend: a campaign of escalated social engineering tactics originally associated with the ransomware group "Black Basta."

Their previous approach involved overwhelming users with email spam, prompting them to create a legitimate help-desk ticket to resolve the issue. The attacker would then contact the end user, posing as the help desk, to respond to the ticket.

In more recent incidents, attackers have advanced their tactics by using **Microsoft Teams** chat messages to communicate with targeted users and incorporating **malicious QR codes** to facilitate initial access.

The underlying motivation is likely to lay the groundwork for follow-up social engineering techniques, convince users to download remote monitoring and management (RMM) tools, and gain initial access to the targeted environment. Ultimately, the attackers' end goal in these incidents is almost certainly the deployment of ransomware.

This rapidly escalating campaign poses a significant threat to organizations. The threat group is targeting many of our customers across diverse sectors and geographies with alarming intensity. The sheer volume of activity is also unique; in one incident alone, we observed approximately 1,000 emails bombarding a single user within just 50 minutes. Due to commonalities in domain creation and Cobalt Strike configurations, we attribute this activity to Black Basta with high confidence.

Tactic Shift—Late October 2024

In incidents during late October 2024, we observed the following changes in Black Basta's tactics, techniques, and procedures (TTPs):

Use of Microsoft Teams Chats

1. After mass email spam events, the targeted users were added to Microsoft Teams chats with external users. These external users operated from Entra ID tenants they created to pose as support, admin, or help-desk staff.

2. The following tenants were observed with the following naming convention "*.onmicrosoft.com". Examples we have seen so far include:

- **securityadminhelper.onmicrosoft[.]com**
- **supportserviceadmin.onmicrosoft[.]com**
- **supportadministrator.onmicrosoft[.]com**
- **cybersecurityadmin.onmicrosoft[.]com**

1. These external users set their profiles to a "DisplayName" designed to make the targeted user think they were communicating with a help-desk account. In almost all instances we've observed, the display name included the string "Help Desk," often surrounded by whitespace characters, which is likely to center the name within the chat. We also observed that, typically, targeted users were added to a "OneOnOne" chat.

What you can do: When hunting within your own environment for similar activity, we recommend searching for Teams display names that feature strings of this nature, rather than just searching for direct matches.

1. Upon investigation, we found that the actions of the external users generally originated from Russia, with the time zone data logged by Teams regularly featuring Moscow.

RMM Shift/QR Codes

In recent incidents, we have also observed the threat actors enticing targeted users to use QuickAssist for the "support" sessions, not just AnyDesk. Additionally, targeted users were sent QR codes within these chats, masquerading as legitimately branded company QR code images.

1. Threat actors are using domains like the following for this QR-code phishing activity:

- **qr-s1[.]com**
- **qr-s2[.]com**
- **qr-s3[.]com**
- **qr-s4[.]com**

1. In each attack, the subdomains of these domains are tailored to match the targeted organization. For example: **companyname.qr-s1[.]com**.
2. We've also observed the creation of more generic subdomains, likely used to target non-specific individuals, rather than specific organizations. An example of a less specific subdomain is: **l1ve.qr-s1[.]com** (note the use of "1" in place of "l").
3. This pattern follows our observations from previous Black Basta campaigns, where the group used domain naming conventions such as, upd7, upd7a, upd10, upd10a.
4. The exact start date of the threat actor's use of QR codes is unclear. However, we tracked the domain details to find older domains created in early October that follow the same naming convention. This suggests they were almost certainly created by the same threat actor with the intention of using QR codes. This indicates that the threat actor likely started using or was planning to use this approach since early October.
5. It is still unclear what the QR codes are specifically being used for. It is realistically possible that the codes direct users to further malicious infrastructure.

Black Basta Email Spam Campaign

We have observed several advertisements on the dark web offering email spam services, which are commonly sold for approximately $10–500. Owing to the tactic's simplicity and low cost, even the least technically sophisticated actors can easily utilize these services.

After spamming end users with emails, attackers followed up with a voice-over-IP phishing (vishing) phone call. During this call, they would attempt to convince the user to download an RMM tool and allow the attacker access to the user's host.Notably, two users were contacted via Teams chat messages by external emails from the domains **supportadminstrator.onmicrosoft[.]com** and **supportserviceadmin.onmicrosoft[.]com**. The attacker posed as a help-desk member and convinced one of the users to download AnyDesk under the guise of stopping the email spam.

Using AnyDesk, the attacker then accessed the users' computers and installed malicious files. These files were named to appear as anti-spam programs, such as "**AntispamAccount.exe**," "**AntispamUpdate.exe**," and "**AntispamConnectUS.exe**." The attacker downloaded the files within five minutes of running AnyDesk. The file "AntispamAccount.exe" accessed the Local Security Authority Service (LSASS), indicating it was used to collect user credentials on the compromised host. In addition, file "AntispamConnectUS.exe" generated network traffic to hundreds of other internal hosts, likely to discover additional resources on the network.

Successful execution of these files led to Cobalt Strike beaconing to domains such as **companymartec[.]com** and **hessetechnology[.]com**. The threat actor likely created these domains to masquerade as legitimate organizations within specific industries. Following this, the Impacket module "secretsdump.py" was run, likely to capture Kerberos password hashes for lateral movement.

The activity was identified and quickly contained and remediated at this stage in the attack, preventing the attack from progressing further in the kill chain.

Email and Teams Spam: What They Have in Common

Observing the indicators associated with the Teams and email spam, we can identify the following insights.

Commonality in Spam Emails:

- The domains used are primarily old and related to e-commerce, finance, or service offerings.
- The email addresses are typically from automated systems or services that send confirmations or notifications (e.g., noreply@domain[.]com, subscription@domain[.]com, support@domain[.]com, help@domain[.]com, marketing@domain[.]com).

Common Email Subjects:

The subject lines of these emails are often similar and include:

- "Your account has been created"
- "Welcome to XYZ"
- "Thank you for registering"
- "Please verify your email"
- "Special offer for you"

How ReliaQuest Is Countering This Threat

We've been actively monitoring the evolution of Black Basta's TTPs. In particular, we are watching closely for external chat events from unusual locations, especially those with display names like "Help Desk" from suspicious external tenants.

We are also continuously tracking the creation of Cobalt Strike domains and adding them to our threat feeds, and monitoring the creation of subdomains associated with QR code phishing. As these subdomains are tailored to match targeted organizations, this gives us a near-real-time view of which organizations and sectors are being targeted.

Recommendations

To safeguard your networks from these threats, we recommend blocking identified malicious domains and subdomains.

- To mitigate against tactics involving Microsoft Teams and QR code phishing, organizations should disable communication from external users within Teams to prevent unwanted chat messages from reaching end users.
- When communication with external users is necessary, specific trusted domains can be allowlisted. Additionally, setting up aggressive anti-spam policies within email security tools can prevent spam from inundating end users' inboxes.
- Ensuring that logging is enabled for Teams, particularly the ChatCreated event, will facilitate detecting and investigating such activities.
- Microsoft Teams accounts impersonating IT help desks typically have their names set to "Help Desk." This string is often surrounded by whitespace characters, likely to center the name within chats. When searching for these accounts, organizations should search for "contains," rather than a direct match.
- The post-exploitation activities linked to these tactics, such as Impacket abuse and the deployment of Cobalt Strike beacons, are neither new nor unexpected. Existing detection rules and security tools are well-prepared to address these threats, enabling organizations to respond effectively to these tactics.

Conclusion

This campaign is still evolving, with Black Basta demonstrating their ability to rapidly adapt their TTPs, likely to thwart defenders and buy themselves more time in networks to further their attacks. While their initial access methods have changed, their post-exploitation activities are likely to remain consistent with previously observed patterns, which are covered by existing security tools and detections rules.

ReliaQuest provides a comprehensive suite of detection rules designed to identify Black Basta activity, enhancing customer resilience against the threat group's evolving TTPs.

There has been a significant rise in ransomware actors using social engineering techniques to gain unauthorized access to sensitive systems and data. Many of these techniques likely leverage native-English speakers, allowing for more convincing and sophisticated phishing messages, therefore significantly raising the likelihood of successfully deceiving targets.

To defend against these threats, organizations should ensure employees remain vigilant against current social engineering tactics by providing ongoing training and awareness programs that highlight the latest attacker threats

and techniques. This vigilance should be paired with a robust defense-in-depth strategy, incorporating multiple layers of security measures such as firewalls, intrusion detection systems, and regular security audits. This approach will help identify and neutralize potential suspicious activity before it can cause any harm. By combining informed and alert employees with comprehensive security protocols, organizations can significantly reduce the risk of successful social engineering attacks and safeguard their critical assets.
