TrickBot teams up with Shatak phishers for Conti ransomware attacks

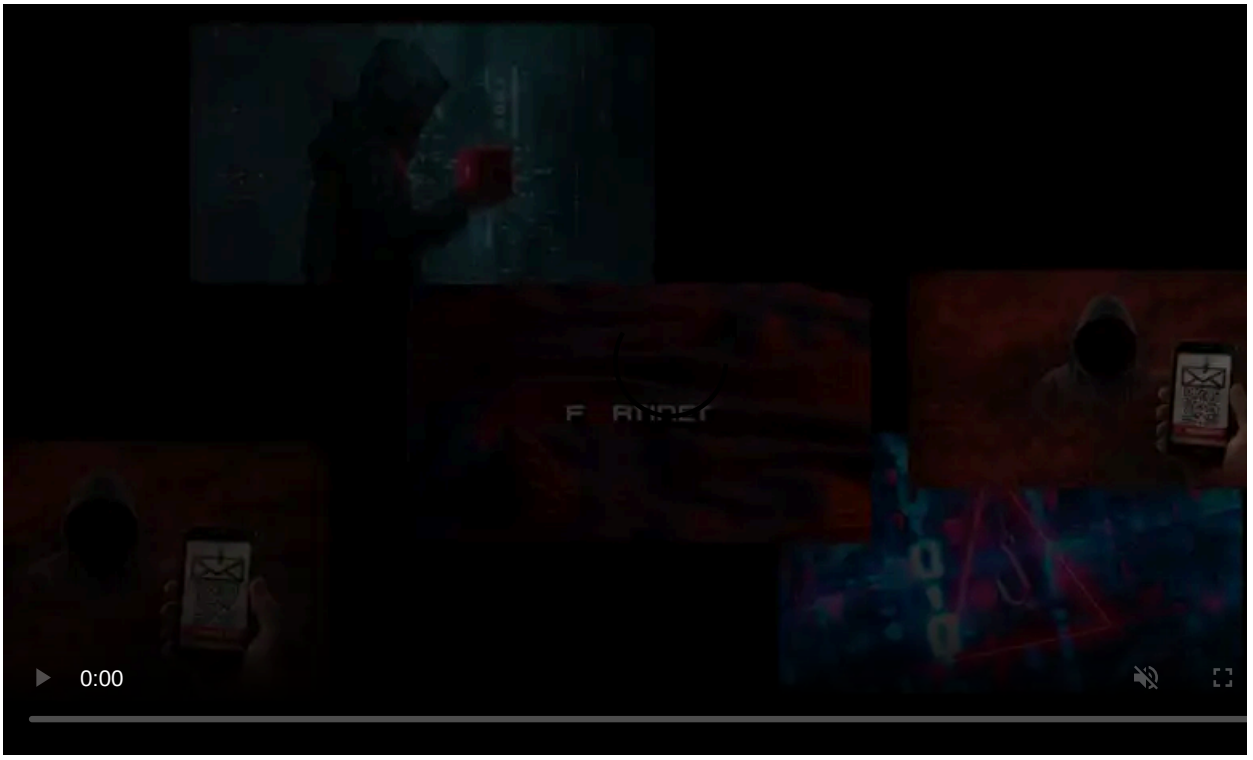
By Bill Toulas

Published: 2021-11-10 · Archived: 2026-04-06 00:04:19 UTC

A threat actor tracked as Shatak (TA551) recently partnered with the ITG23 gang (aka TrickBot and Wizard Spider) to deploy Conti ransomware on targeted systems.

The Shatak operation partners with other malware developers to create phishing campaigns that download and infect victims with malware.

Researchers from IBM X-Force discovered that Shatak and TrickBot began working together in July 2021, with what appears to be good results, as the campaigns have continued until today.

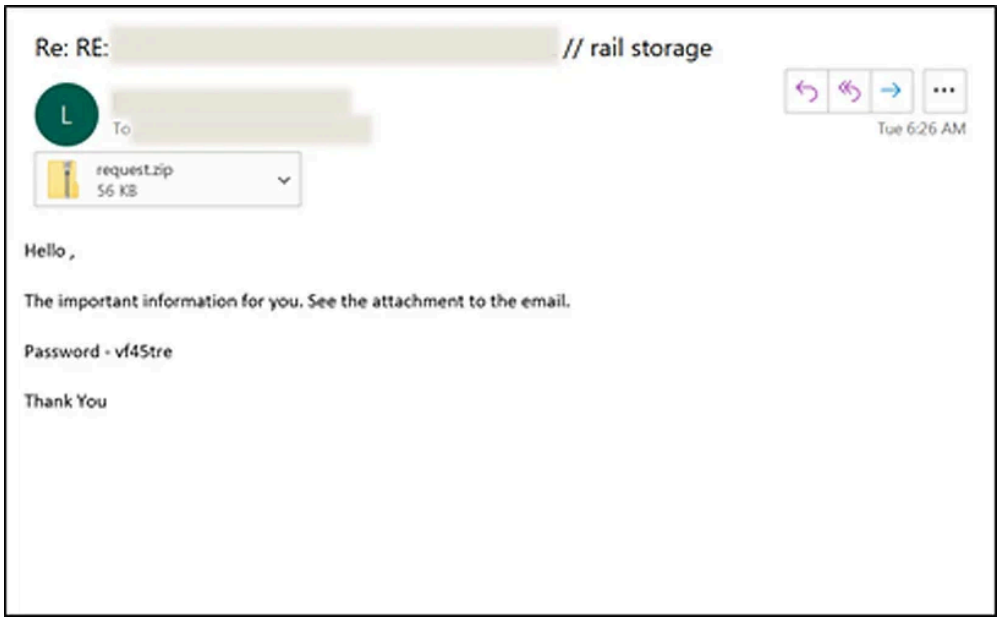

0:00

A recent technical analysis from Cybereason provides more details on how the two distinct actors partnered to deliver ransomware attacks.

Attack starts with a phishing email

A typical infection chain starts with a phishing email sent by Shatak, carrying a password-protected archive containing a malicious document.

According to an October report by IBM X-Force, Shatak commonly uses reply-chain emails stolen from previous victims and adds password-protected archive attachments.

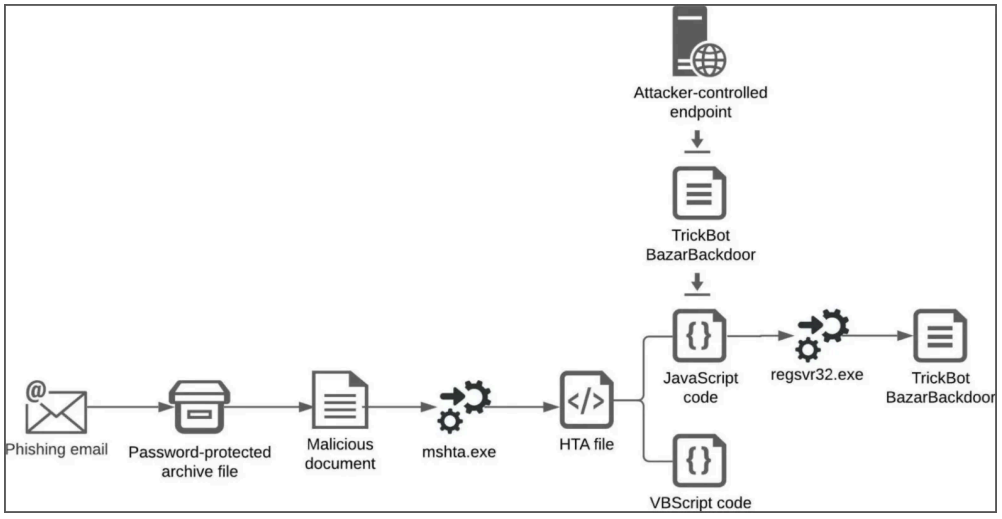


Example Shatak phishing email

Source: IBM X-Force

These attachments contain scripts that execute base-64 encoded code to download and install the TrickBot or BazarBackdoor malware from a remote site.

The distribution sites used in the most recent campaign are based in European countries such as Germany, Slovakia, and the Netherlands.



Shatak's infection chain

Source: Cybereason

After successfully deploying TrickBot and/or BazarBackdoor, ITG23 takes over by deploying a Cobalt Strike beacon on the compromised system, adding it to the scheduled tasks for persistence.

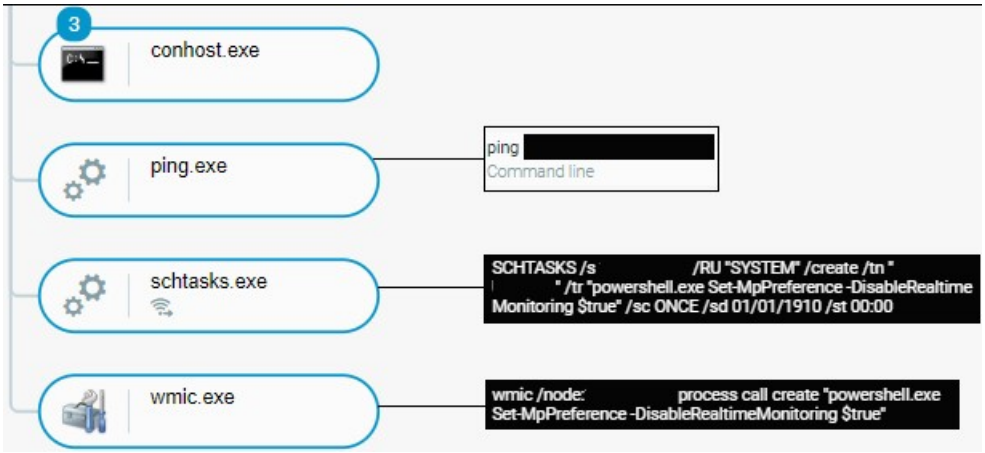
The Conti actors then use the dropped BazarBackdoor for network reconnaissance, enumerating users, domain admins, shared computers, and shared resources.

Then they steal user credentials, password hashes, and Active Directory data, and abuse what they can to spread laterally through the network.

Some signs of this activity include fiddling with registry values that enable the RDP connectivity and modifying Windows Firewall rules with the 'netsh' command.

Windows Defender's real-time monitoring feature is also disabled to prevent alerts or interventions during the encryption process.

The next step is data exfiltration, which is the final stage before the file encryption, with Conti using the 'Rclone' tool to send everything to a remote endpoint under their control.



Conti disabling Defender's real-time protections.
Source: Cybereason

After harvesting all valuable data from the network, the threat actors deploy the ransomware to encrypt devices.

Other potential collaborations

In a recent report from France's Computer Emergency Response Team (CERT), TA551 appears as a collaborator of 'Lockean', a newly discovered ransomware group with multiple affiliations.

In that case, Shatak was sending phishing emails to distribute the Qbot/QakBot banking trojan, which was used for deploying the ProLock, Egregor, and DoppelPaymer ransomware infections.

As such, TA551 may have more collaborations with other ransomware gangs besides those spotted by analysts.

This threat actor is also identified under different names, such as Shathak, UNC2420, and Gold Cabin.

How to protect yourself

The best defense against these types of attacks is to train employees on the risks of phishing emails.

Apart from that, admins should enforce the use of multi-factor authentication on accounts, disable unused RDP services, and regularly monitor the relevant event logs for unusual configuration changes.

Finally, an important safety measure is regularly backing up important data to a secured remote location and then taking those backups offline so they can't be targeted by threat actors.
