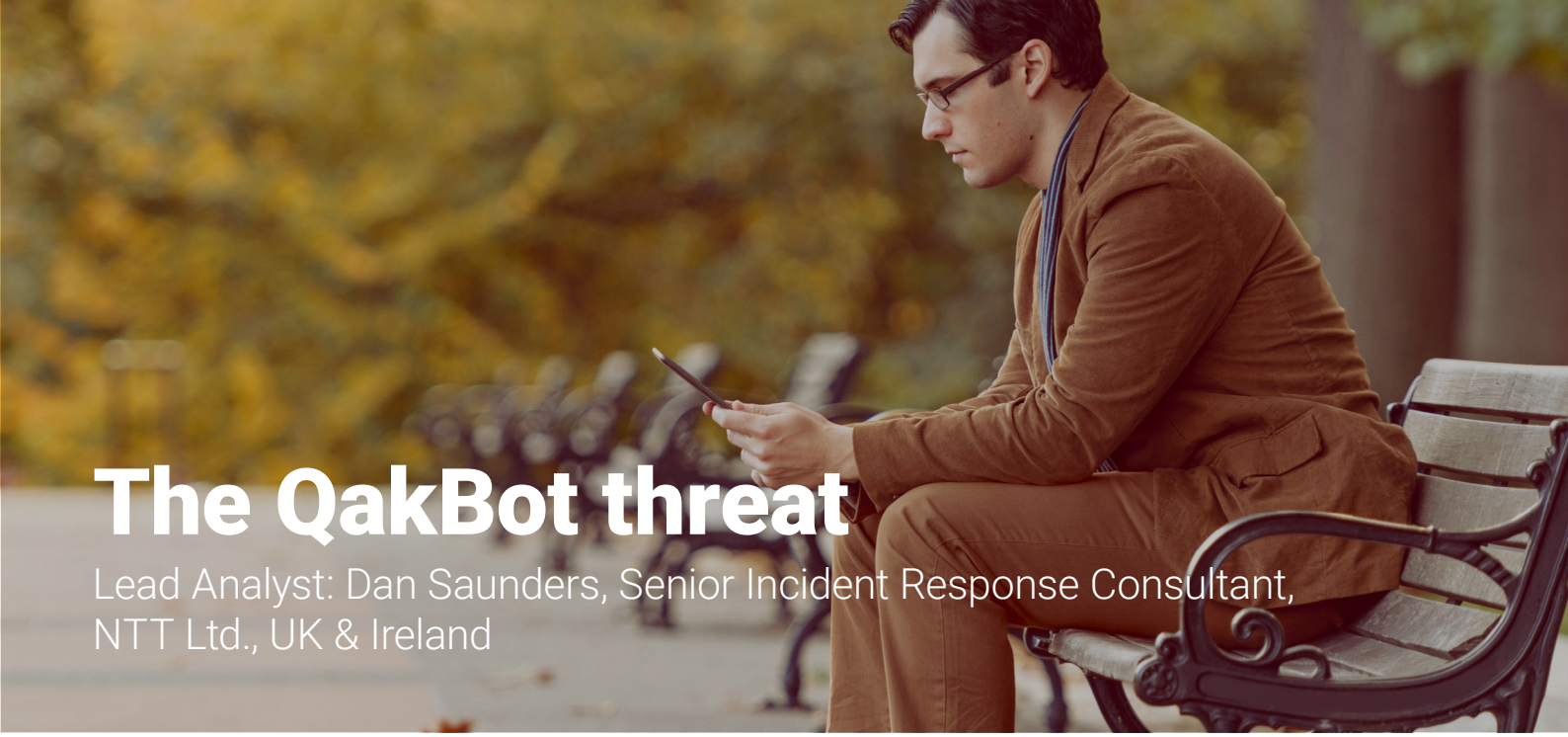
Global Threat Intelligence Center

Monthly Threat Report

December 2020

Contents



The QakBot threat

Lead Analyst: Dan Saunders, Senior Incident Response Consultant, NTT Ltd., UK & Ireland

Malspam campaigns distributing QakBot are on the rise and it's not just the banking trojan you should be worried about!

What is QakBot?

QakBot aka Qbot aka Pinkslipbot is a banking trojan aimed at stealing credentials, hunting for financially-related information and recording system keystrokes. Qbot was first discovered in 2008, and has always been a well-structured, multi-layered piece of malware which continues to expand capabilities with every evolution. While it was previously distributed by another infamous banking trojan, Emotet, during 2020, Qbot has been prolific at infecting numerous organizations during its own relentless campaigns, which inevitably result in unauthorized access to the victim's infrastructure. Qbot is currently being actively supported, with new versions typically being issued monthly.

Initial attack vector

Our Digital Forensics Incident Response (DFIR) team has responded to incidents involving Qbot to mitigate these types of cyberattacks. The initial attack vector is via widespread malspam campaigns, where malicious emails entice unsuspecting victims to access a URL link to download an archive (.ZIP) file. Within the attachment is an obfuscated visual basic script (.VBS), which once executed makes HTTP(S) requests to compromised websites. If the website is reached, it attempts to download one of several first stage payloads. The payloads often have an image file (.PNG) extension, however they are actually executable.

```
http://restaurantbrighton[.]ru/uyqcb/88888888.png
http://royalapartments[.]pl/vtjwwoqxaix/88888888.png
http://alergeny.dietapacjenta[.]pl/pgaakzs/88888888.png
http://egyorg[.]com/vxvipjfembb/88888888.png
```

Figure 1: Example of delivery URLs de-obfuscated from VBScript

Qbot actively harvests email threads from infected environments. These stolen emails are analysed and integrated into future malspam campaigns to make it appear as if the new email is part of an existing valid email conversation. This has the potential to make the next round of campaigns even more effective than the previous, especially when used in a targeted manner.

While Qbot has been detected in a wide variety of industries, it has been most commonly observed in government, manufacturing, military and healthcare organizations.

Qbot operations

The downloaded binary itself is packed and contents are encrypted to deter security researchers from reverse-engineering the malware.

Since Qbot is polymorphic, it is a difficult trojan to contain. First of all, the malware binary masks itself as the legitimate **calc.exe** program to avoid detection and secondly carries out process injection into **explorer.exe**. This process is then used to carry out additional injection and execute even more malicious functions. Some of the most notorious are hooking, credential stealing, keylogging, email collection and brute-force password capabilities. Persistence is maintained via the use of the Windows registry start-up run key and scheduled task creation.

A typical directory containing the main Qbot binary (packed), configuration data and other modules is depicted below.

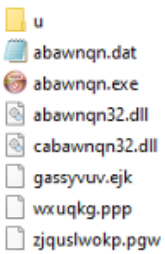


Figure 2: QakBot %APPDATA% Directory

The DoppelPaymer connection

As if malware infection isn't bad enough, Qbot operators are collaborating with 'big-game' ransomware groups to permit access to compromised enterprise networks for a secondary ransomware attack. This supports the current trend observed with commodity malware families branching out to facilitate themselves as droppers for other threat actors.

During our incident response engagements, we've identified significant traces of Qbot throughout compromised networks, following successful privilege escalation and lateral movement using harvested compromised credentials. This is of significance, as at this stage, in parallel within the network traffic, we observed command and control (C2) infrastructure communication associated to DoppelPaymer. Cobalt Strike beacons were subsequently created on domain controllers, not only reverse-shells in memory, but also leveraging admin shares to host the beacons in binary form and perform lateral movement.

Organizations have opportunities to detect domain discovery activities by monitoring common sysadmin tools and command and control (C2) within the PowerShell logs. While the malicious code is often obfuscated, it can be decoded, revealing the C2 infrastructure.

Obfuscated code is layered as follows; first layer Base64 UTF-16LE (Unicode) > second layer Base64 UTF-8 + GZip Compressed > third layer Base64 UTF-8 + exclusive OR (XOR).

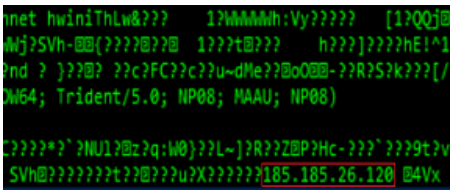


Figure 3: Shellcode snippet revealing C2

This enables DoppelPaymer to carry out domain discovery to gather target information, identify backup servers to prevent restoration, target file servers for data exfiltration and then encrypt the victim's data for impact. In the end, the victim is left with a substantial ransom demand, or face having their data permanently locked, sold on the dark web or published.

Mitigation recommendations

- Scan URLs embedded into emails from external domains for malicious indicators.
- Block VBScripts and JavaScripts from launching downloaded executables.
- Ensure local 'Administrator' account passwords are complex.
- Proactively monitor and threat hunt, leveraging endpoint detection response (EDR) for process injection and suspicious PowerShell execution.
- Monitor web proxy logs and firewall logs to detect anomalies and apply threat intelligence to identify command and control (C2) communication.

Using QakBot, stolen emails are analysed and integrated into future malspam campaigns to make it appear as if the new email is part of an existing valid email conversation. **This can make the next round of campaigns even more effective than the previous.**

#Spotlight 1

Ransomware as-a-service becomes increasingly accessible via social media and open sources

Lead Analyst: Insikt Group, Recorded Future*

Hackers don't need to search the dark web for access to their own ransomware platforms these days. Cybercriminals are continually finding new ways to promote their underground businesses and gain the attention of new customers and novice hackers.

Several threat actors have recently taken to popular social media and open sources like YouTube, Vimeo, and Sellix to advertise and demonstrate their discount-priced USD 40 ransomware as-a-service (RaaS) builder called ZagreuS.

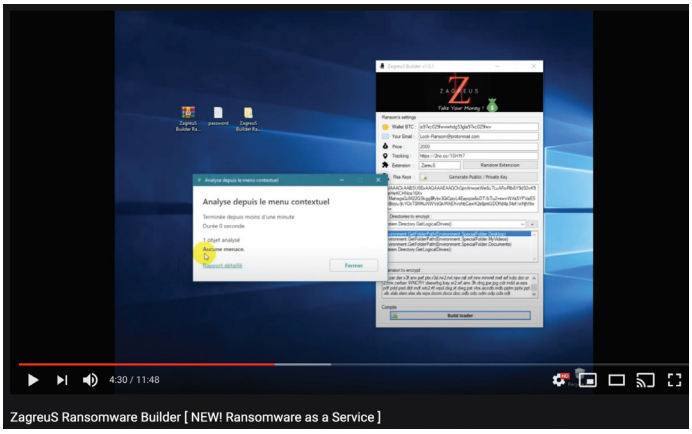


Figure 4: YouTube video demonstration of the ZagreuS ransomware builder. (Source: Recorded Future)*

The ZagreuS ransomware offers several attractive and easy-to-use features that make it accessible and manageable for low-level beginner hackers.

According to the sellers, the ransomware features include:

- Asymmetric encryption, using a hybrid combination of AES-256 and RSA-2048 algorithms to lock files on the target machine.
- It deletes shadow copies and is claimed to encrypt files at a very high speed.
- Claims to bypass UAC.
- Built-in loader that can be customized to drop additional payloads such as RATs (remote-access trojans).
- The attacker can monitor the number of victims infected with the ransomware.
- Easy personalization. Enter your contact information and bitcoin address for fast payment.

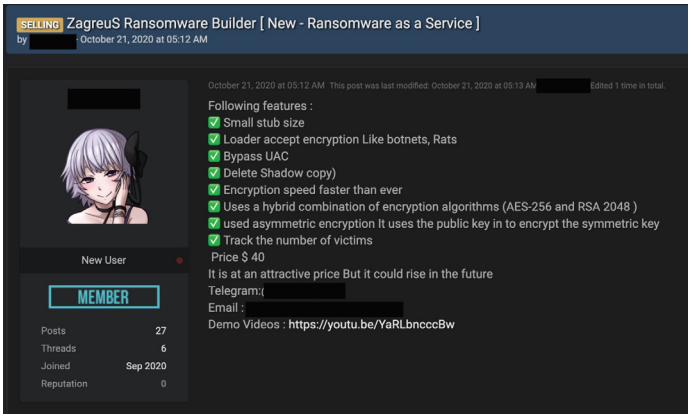


Figure 5: A new user advertised the ZagreuS features on a deep web hacking forum. (Source: Recorded Future)*

According to the original seller, ZagreuS is designed for attacking larger networks of companies, enterprises and hospitals. The 11-minute demo video posted on YouTube describes that the seller will receive a 30% commission for each ransom collected, while the remaining 70% is kept by the operator/buyer. The ransomware builder is currently trending at a low price of USD 40, paid in cryptocurrency to the seller's wallet.

Several interested buyers left comments on the sale posts on underground forums inquiring if anyone had tested the ZagreuS builder and expressed interest in trying it out. Typically, in these instances, the low price of the builder is an indication that the seller lacks experience or that the tool isn't very valuable. Insikt Group has found that most often, the tool does not function well, can be easily decrypted and it can be very difficult for the 'affiliate' criminals to make a profit off of their victims.

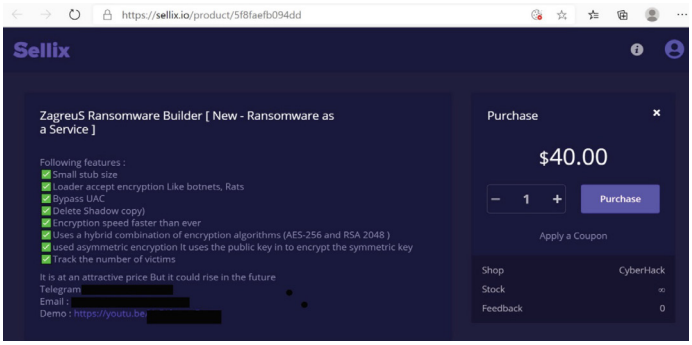


Figure 6: This threat actor cross-posted their advertisement for ZagreuS ransomware builder on YouTube and Sellix.io

Many online platforms and social media applications are aware of these advertisements and work to have them removed. When this particular demo video was removed from the original YouTube channel, the threat actor quickly uploaded it again under a different link and pivoted to other platforms for clear web and deep web marketing, including sellix.io, RAID forums, hackforums and Github.

Ransomware variant coverage by year

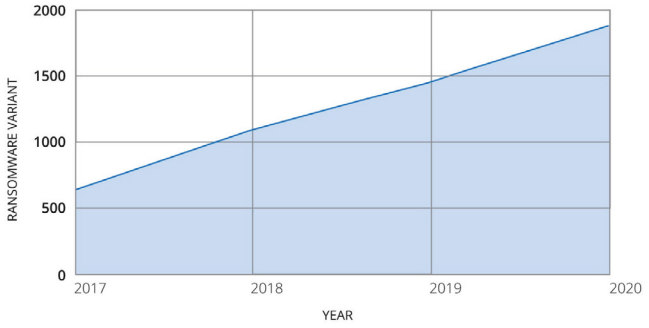


Figure 7: Year-on-year ransomware variant coverage (Source: Recorded Future)*

Ransomware has stolen the cybercrime stage in the past year, quickly becoming one of the most damaging and prevalent forms of cyberattacks. Industries such as state and local government, healthcare and finance have taken an especially hard hit from ransomware attacks in the past year, and it doesn't appear to be slowing down. There are currently over 1,800 variants of ransomware, with the top 45 variants bringing in the most ransom money.

Although the barrier of entry for threat actors to get into ransomware has been lower than ever, very few criminals make a profit off of these low-cost, simple RaaS tools. However, those that are successful have taken advantage of the situation and have increased ransom demands. Some are even practicing double exploitation of their victims -demanding a ransom and still releasing the victims' personal data for sale on underground forums after they have paid.

** Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams in reducing exposure by uncovering unknown threats and informing better, faster decisions. For more information, see here.*

Phishing continues to be a **prominent threat vector**

Lead Analyst: Jon Heimerl, CISSP, Sr. Manager,
Global Threat Intelligence Center, US

Phishing attacks have long been one of the most popular threat vectors used by attackers. Simple in concept, a phishing attack is a hostile email designed to facilitate the threat actor's attack. This can be the delivery of a malware attachment, redirection via a malevolent link in the email, a request to take some action (like in a business email compromise attack), or simply to engage in the gathering of information (like harvesting valid email addresses) in preparation for future attacks. The combination of potential uses means that phishing attacks are actually far from simple.

A phishing email can be a customized, one-off email, manually built by an attacker for a very specific attack against a particular target, and it can be one of millions of phishing emails sent via a malspam campaign run through a botnet. In many cases, the results of the phishing attack depend on how targeted, or appropriate, the email is for the intended audience. In most analyses of phishing attacks, it appears victims open about a third of phishing emails and click through them about 10% of the time. In phishing attacks I have conducted myself (in tests with clients who contracted for the test), with a small amount of customization, I reached as high as a 100% open rate and about a 67% click-through rate. If you consider that a dedicated malspam campaign can send millions of emails, the potential impact those volumes could have on most organizations should be intimidating.

Why do phishing attacks work?

A successful phishing attack is the result of two primary factors: the volume of the emails sent and the attractiveness of the lure.

Volume is often important because of the open and click-through rates. If the numbers above are accurate (33% open and 10% of those click) it means about 3.3% of phishing emails are likely to result in a click to download malware or be directed to a hostile website with an exploit kit. If the numbers are close, that means a malspam campaign which sends 1,000 emails might expect to reach something on the order of 33 click-throughs. But a malspam campaign which sends a million emails might expect more like 33,000 click-throughs.

If the attacker can increase both chances – the chance of an open and the chance of a click-through – by using an attractive lure, this gets even worse. The lure is the topic of the phishing email – intended to grab the attention of the recipient, and lure them into being interested, and as a result, opening and clicking into the email. Lures can come in various forms, but some of the more popular and timely lures includes emails with subject lines like those shown in Table 1. It's worth noting that this isn't a complete list, but does include many of the more popular and timely subject lines observed in phishing emails in the final quarter of the 2020 calendar year. And, just because an email has one of these subject lines it doesn't guarantee it is a phishing email, but it should probably be looked at with at least some suspicion. (Misspellings, punctuation errors, random characters and other errors shown as copied from suspect emails.)

Phishing campaign emails **tend to have subject lines with misspelled words,** grammatical or punctuation errors or include random characters out of context.

Focus of lure	Subject lines in support of lure
COVID-19 related – to capitalize on general interest in COVID-19, current infections, financial assistance and vaccines	URGENT INFORMATION LETTER: COVID-19 NEW APPROVED VACCINES
	SBA Application – Review and Proceed
	Update on the Coronavirus Vaccine
	Important Covid-19 Updates
	COVID-19 Everything you need to know
	COVID-19 Relieve
Home security – to capitalize on feelings of unease in communities	$850 WORTH OF SECURITY EQUIPMENT FREE
	Be Safe Today with a Monitored System from Protect Your Home
	Home Security with SmartHome monitoring offer
	Get a $100 Visa Rewards Card from Protect Your Home
Computer security – to capitalize on uncertainty about attacks and viruses	Last reminder, Your Antivirus expires in 24 hr
	Your <company> subscription has expired ! Please respond!
Healthcare insurance – to capitalize on open enrollment periods	Your ref. NO. _965658 (regarding Medicare or insurance updates)
	Get Health Insurance Quotes Online
	Enroll in a Health Plan Before the Deadline
	2021 Open Enrollment is Here!
Holiday season – to capitalize on online shopping demand	PS5s available now
	Special Sale Price on Playstation 5
	Receive the new Ipad Pro
Banking – to capitalize on financial uncertainty	Your account will be restricted if you fail to update
	Give Us Your Opinion about <bank> And We'll Give You a $50-Vaule Gift!
	Online Banking Alert®
	Quick order confirmation (regarding a PayPal purchase)
	PayPal Policy Updates
Shipping – to capitalize on gratification and anticipation	RE: Your order #633-2913 has shipped
	Delivery status change
	Your package could not be delivered
Political – to capitalize on frustrations with US elections	The President needs you.
	Election interference
	Voter registration details couldn't be confirmed
Online accounts – to capitalize on anxiety over attacks and access	Re. Current update to your Apple ID – Your account has been temporary locked
	Re: Important – Your Amazon account statement is available: Your account on hold :
	Update your Apple ID account when you're ready
	Your Netflix cancellation confirmation
Attempted access to internal systems – to capitalize on user familiarity with organizational tools	There's new activity in Teams
	Your Outlook Mailbox Will Shutdown Verify Your Account
	Email Verification Required
	Your Microsoft account password has expired

Table 1: Sample email subject lines of phishing attack lures

Summary

Phishing campaigns will continue to be a problem for one simple reason – they work. There are technical solutions which can reduce the amount of spam and malspam which reach employees. Good spam filters can catch even some targeted phishing emails. And employees should be restricted to operate – browse the web and process email – from non-privileged accounts, but ultimately, the final filter is the employees themselves.

This means good phishing awareness is one of the best defenses an organization can have against phishing attacks. Users should have a comfortable awareness of how to identify phishing attacks. Often, even a cursory comparison of the subject line, email contents and the address of the sender, can reveal fake or malicious emails. An email with a subject line about an account lockup, with email contents about the victim's bank, and a sending email of adavant3434@monster.com should make it obvious to most users that the email isn't genuine, but not all phishing emails are this easy to identify.

In the final quarter of 2020, users can assume that any email which includes 'vaccine' or 'Playstation 5' in the subject line has a high probability of being fraudulent, just as emails which include unsolicited or unexpected links to DocuSign or DropBox. The subjects in the above table are representative of some of the more common lures being used now. There may of course be some variations in the text, but common lures are often similar. If users are at least familiar with these lures and subjects which phishing attacks are currently using, it can improve your organization's resistance to such phishing attacks.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

Our 2020 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.


NTT