HC3 Analyst Note
April 8, 2024 TLP:CLEAR Report: 202404081500

Analysis of the BazaCall/BazarCall Phishing Method

Executive Summary
Operating since as early as 2000, the threat actors behind BazaCall (also known as BazarCall), an advanced social engineering method, have been observed using multiple tactics, techniques, and procedures (TTPs) to breach targeted networks and lure unsuspecting victims into downloading its malicious malware. Many of these threat groups are offshoots of the defunct, notorious Russia-linked Conti gang, known to have aggressively targeted the Healthcare and Public Health (HPH) sector. Over time, these groups have since adopted and independently developed their own targeted phishing tactics that continuously evolve to target victims. What follows is an overview and examination of these groups, their TTPs, their target industries and victim countries, impact to the HPH sector, indicators of compromise, and recommended defense and mitigations.

Overview of BazaCall
The BazaCall method, also referred to as call-back phishing, emerged in late 2000 as an attack vector used by the Ryuk ransomware operation. BazaCall can be both a ransomware and data exfiltration attack that are used together to increase pressure on and damage to a victim. The operators behind the BazaCall phishing method have since continued to evolve with updated social engineering tactics to deploy malware on targeted networks. The switch to social engineering was caused by the predictability of previous attack methods, which caused threat actor profits to dwindle as defenders started to enforce effective mitigations. However, tricking humans would allow for a more flexible approach that could change from one campaign to another, making attacks more difficult to identify and defend against.

An Israeli cybersecurity company known to track the TTPs of threat groups that utilize BazaCall published an internal communique from a previous Conti member. The Conti member stated: “We can’t win the technology war because on this ground we compete with billion-dollar companies, but we can win the human factor.” As such, the threat actors that utilize this tactic target employees, whether from one company or an entire industry, and tailor the phishing campaigns accordingly for maximum efficiency.

Technical Details
BazaCall campaigns begin with an e-mail that uses various social engineering lures to trick target recipients into calling a phone number. For example, the e-mail 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 e-mails 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 e-mail does away with the subscription trial angle and instead poses as a confirmation receipt for a purchased software license.

Unlike typical spam and phishing e-mails, 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. It is 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. This lack of typical malicious elements – links or attachments – adds a level of difficulty in detecting and hunting for these e-mails. In addition, the messaging of the e-mail’s content might also add an air of legitimacy if the user has been narrowly trained to avoid typical phishing and malware e-mails, but not taught to be wary of social engineering techniques.

HC3 Analyst Note

April 8, 2024 TLP:CLEAR Report: 202404081500

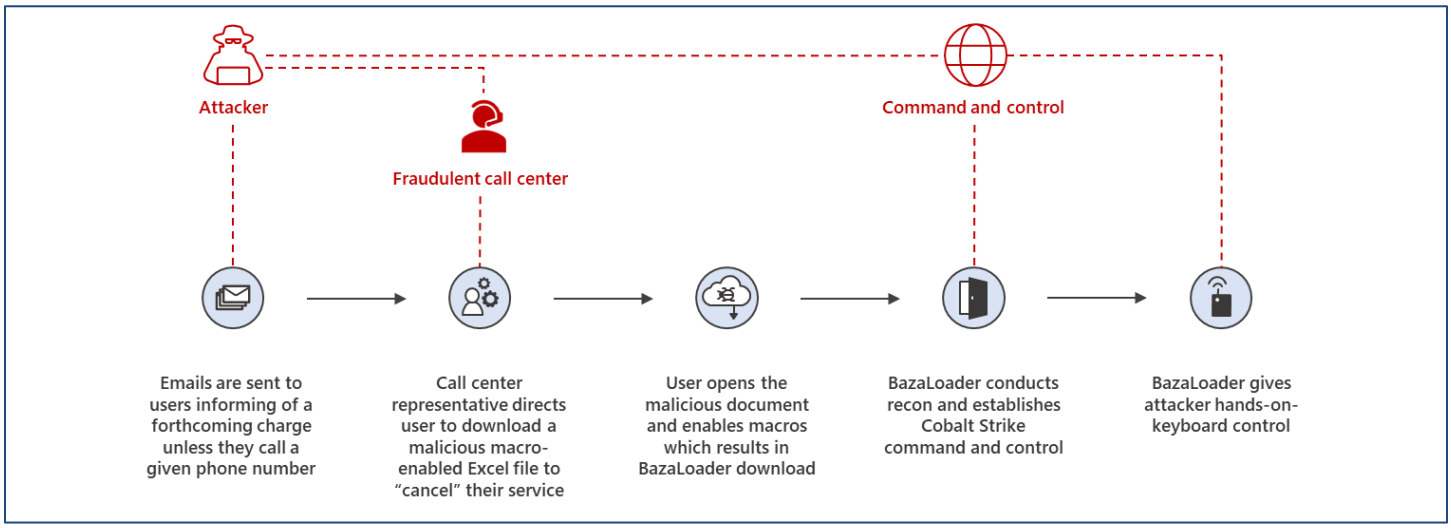


Figure 1: The flow of a typical BazaCall attack, from the spam e-mail to social engineering to the payload being downloaded and hands-on-keyboard attacks. *(Source: Microsoft Security)*

Each BazaCall e-mail is sent from a different sender, typically using free e-mail services and likely-compromised e-mail addresses. The lures within the e-mail 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 e-mail'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:

Sample Subject Lines in BazaCall Phishing Tactics
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 e-mail contains unique ID number]
Thanks for deciding to become a member of BooyaFitness. Fitness program was never simpler before [body of e-mail 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 e-mail 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.

If a target recipient does decide to call the phone number indicated in the e-mail, 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 or convinces them to start a remote access session via legitimate software controlled by a network intruder.

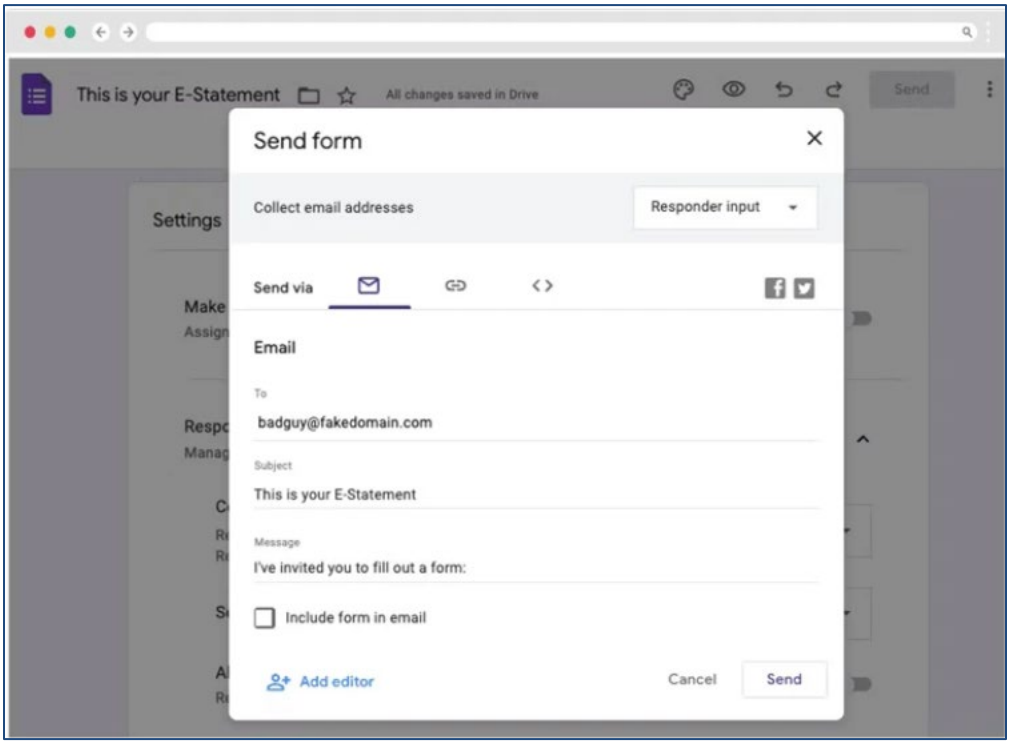


Figure 2: Sample Google Forms phishing campaign. *(Source: The Hacker News)*

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 e-mail. For example, an e-mail claiming that a user's free trial for "Pre Pear Cooking" was set to expire was paired with the domain, "topcooks[.]us".

At the height of the COVID-19 pandemic, BazaLoader, the loader used to deploy ransomware or other types of malware, masqueraded as a fake movie-streaming service known as BravoMovies. During this period, subscriptions to online streaming services skyrocketed, surpassing one billion users globally in 2020. Using entertainment subscription themes was a timely and effective method for convincing users to engage with the e-mail content and follow-on malicious documents. In a growing trend of users cancelling online entertainment following the industry's growth spurt during the COVID-19 pandemic, threat actors utilizing BazaCall took advantage of this human behavior trend in an identified campaign.

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. According to the Microsoft Threat Intelligence Team, 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.

More recently, cybersecurity researchers have observed these threat actors leveraging Google Forms to lend the scheme a veneer of credibility. This method is an attempt to elevate the perceived authenticity of the initial malicious e-mails. By 2023, some of the more popular services that were impersonated included Netflix, Hulu, Disney+, Masterclass, McAfee, Norton, and GeekSquad. It is worth noting that the form has its response receipts enabled, which sends a copy of the response to the form respondent by e-mail, so that the attacker can send an invitation to complete the form themselves and receive the responses. By sending e-mails from a trusted domain, threat actors have a higher change of bypassing secure e-mail gateways.

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.

Known Threat Actors

Conti

First observed in 2019, Conti is a Russian-speaking Ransomware-as-a-Serivice (RaaS) group connected to more than 400 multi-sector cyberattacks, three-quarters of which were based in the United States. Notorious for their aggressive tactics and large-scale attacks, they were known for demanding ransoms as high as $25 million. Often conducting double extortion, they relied on affiliates to target organizations with more than $100 million in annual revenue. However, previously leaked chats showed that some Conti members began to question the targeting of the healthare sector, especially during the height of the COVID-19 pandemic. This led to speculation that there might be a fracturing within the group. Subsequently, following a multi-government sting operation in February 2022, the group disbanded, splintered into smaller groups, and rebranded to evade law enforcement. Despite the shutdown of the Russian-speaking threat group, Conti operators remain active and collaborative in new factions.

For additional information on the Conti threat group, see four previous HC3 reports: Overview of Conti Ransomware, Conti Ransomware Amplify Alert, Conti Ransomware (Update), and Conti Ransomware and the Health Sector.

BazaCall came under the spotlight in 2000 when it was put to use by operators of Ryuk ransomware, which later rebranded into Conti. At least three distinct threat groups – Silent Ransom, Quantum, and Roy/Zeon – all of which split from Ransomware-as-a-Service (RaaS) group, Conti, are known to utilize the BazaCall technique of call-back phishing as an initial access vector to breach targeted networks. The same Israeli cybersecurity company noted that "…call back phishing was the tactic that enabled a widespread shift in the approach to ransomware deployment" and the "attack vector is intrinsically embedded into the Conti organizational tradition."

Silent Ransom

Silent Ransom, also tracked as Luna Moth, was the first derivative group to move away from Conti in

March 2022, and has since been linked to a string of data extortion attacks that entail gaining initial access through subscription expiry e-mails that claim to notify users of pending payment for Zoho Masterclass and Duolingo services. Over three months, the group targeted at least 94 organizations, focusing only on stealing data and extorting the victims. The group has a heavy focus on entities in the HPH sector, with annual revenue between $500,000 and more than $100 billion, almost 40% of them with revenue above $1 billion.

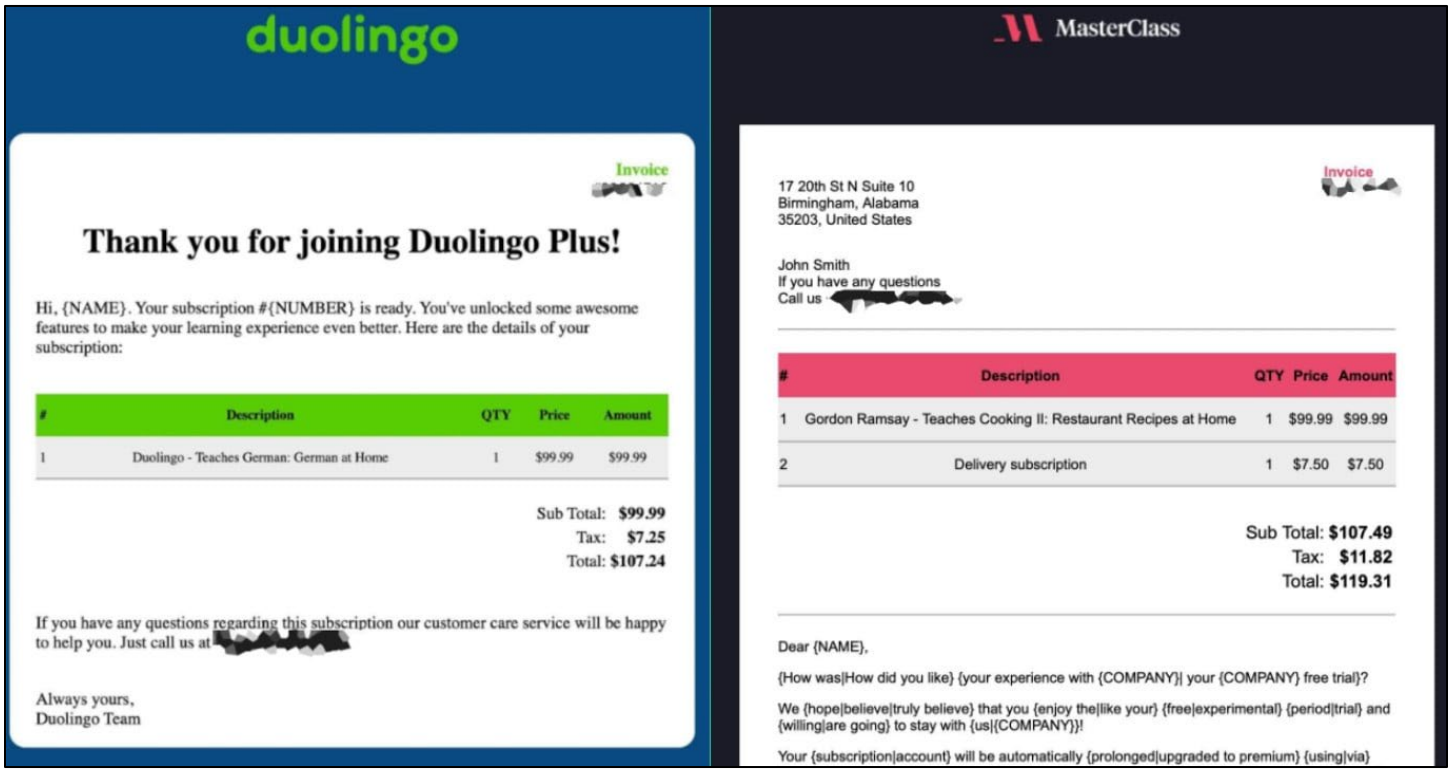


Figure 3: Sample Silent Ransom Phishing E-mails (Source: BleepingComputer)

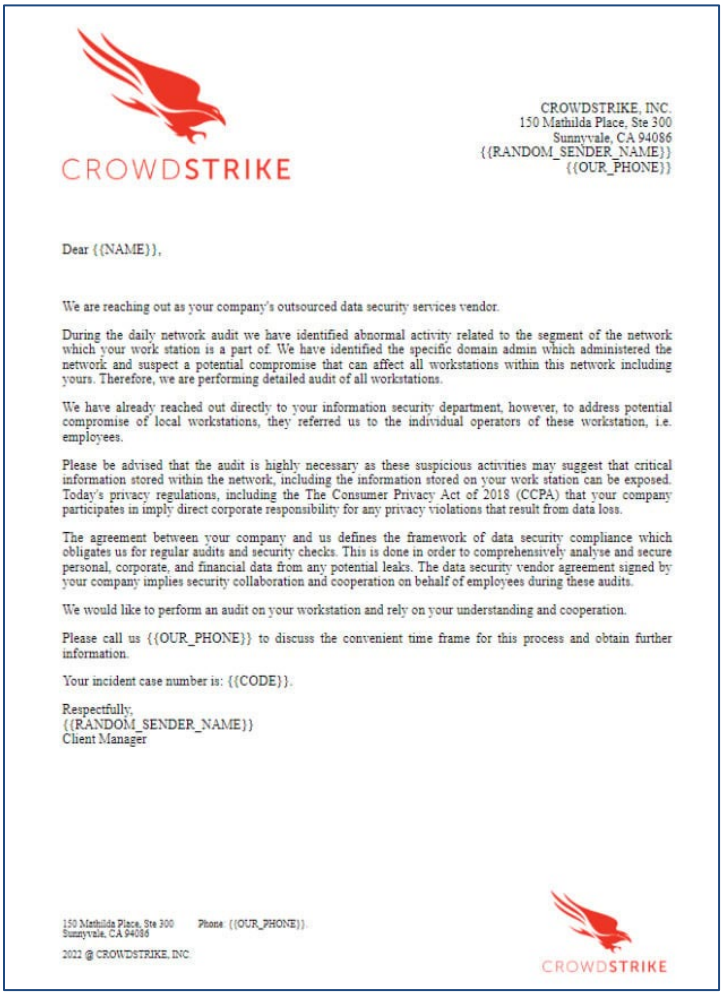
The success of Silent Ransom's highly specified phishing operations have also prompted two other Conti spin-offs, namely Quantum and Roy/Zeon, to follow the same approach starting mid-June 2022, while simultaneously giving their own spin.

Quantum

Quantum started employing their version of BazaCall in an operation named Jörmungandr, the word given to a famed serpent in Norse mythology. The actors developed the operation by hiring individuals specialized in spamming, OSINT, design, and call center operators. Quantum ransomware operators were the main Conti subdivision (Conti Team Two), a group of highly-skilled hackers responsible for breaching the government of Costa Rica in May 2022. Quantum ransomware emerged as a rebranded MountLocker in September 2021, but did not achieve much success. As Conti began to shut down, the Quantum ransomware operation was taken over in April 2022 by the hackers in Conti Team Two, who kept the name from the original operators.

The BazaCall call campaigns attributed to the Quantum group grew more sophisticated over their initial two months in operation, and targeted high-profile companies based on exclusive e-mail datasets they

purchased. Unlike Silent Ransom, which uses falsified e-mails imitating subscription notices as a lure, Quantum's "increasingly sophisticated" spam campaigns are known to proliferate via missives impersonating brands like Oracle and CrowdStrike. Regardless of the theme in the phishing e-mail, the threat actor urged recipients to call a number for further clarifications.



CROWDSTRIKE

CROWDSTRIKE, INC.
150 Mathilda Place, Ste 300
Sunnyvale, CA 94086
{{RANDOM_SENDER_NAME}}
{{OUR_PHONE}}

Dear {{NAME}},

We are reaching out as your company's outsourced data security services vendor.

During the daily network audit we have identified abnormal activity related to the segment of the network which your work station is a part of. We have identified the specific domain admin which administered the network and suspect a potential compromise that can affect all workstations within this network including yours. Therefore, we are performing detailed audit of all workstations.

We have already reached out directly to your information security department, however, to address potential compromise of local workstations, they referred us to the individual operators of these workstation, i.e. employees.

Please be advised that the audit is highly necessary as these suspicious activities may suggest that critical information stored within the network, including the information stored on your work station can be exposed. Today's privacy regulations, including the The Consumer Privacy Act of 2018 (CCPA) that your company participates in imply direct corporate responsibility for any privacy violations that result from data loss.

The agreement between your company and us defines the framework of data security compliance which obligates us for regular audits and security checks. This is done in order to comprehensively analyse and secure personal, corporate, and financial data from any potential leaks. The data security vendor agreement signed by your company implies security collaboration and cooperation on behalf of employees during these audits.

We would like to perform an audit on your workstation and rely on your understanding and cooperation.

Please call us {{OUR_PHONE}} to discuss the convenient time frame for this process and obtain further information.

Your incident case number is: {{CODE}}.

Respectfully,
{{RANDOM_SENDER_NAME}}
Client Manager

150 Mathilda Place, Ste 300 Phone: {{OUR_PHONE}}
Sunnyvale, CA 94086

2022 @ CROWDSTRIKE, INC

CROWDSTRIKE

Figure 4: Quantum impersonates cybersecurity company, CrowdStrike. *(Source: BleepingComputer)*

Quantum has been known to use Jörmungandr to target five "large-scale companies" with annual revenue of more than $20 billion, most of them in the HPH sector. One of those companies was a managed service provider that would have allowed access to hundreds of businesses and put them at risk of being encrypted. When they obtained access to the victim network, Quantum hackers typically stole data and encrypted the systems.

Roy/Zeon

The third group that splintered from Conti and adopted BazaCall-like techniques is referred to as Roy/Zeon, after the names of the two lockers (Roy and Zeon) that they use to encrypt victim networks. This group originated from old members of Conti's "Team One," responsible for the creation of Ryuk itself. They have demonstrated an extremely selective targeting approach, typically favoring companies with high average revenue. The same Israeli cybersecurity company states that Roy/Zeon is the most skilled social

engineer of the three groups, and has the largest number of interchangeable and adjustable Indicators of Compromise (IOCs) and impersonation schemes that it selects from based on its target. Of note, one previous HPH victim of Roy/Zeon included a leading Italian producer of pharmaceuticals.

Impact to the Healthcare and Public Health Sector

Silent Ransom and Quantum, two threat groups known to utilize BazaCall, have a heavy focus on targeting entities in the HPH sector. Previously observed phishing e-mails from BazaCall threat actors used ficticious HPH organization names such as “Medical Reminder Services, Inc.,” “iMed Service, Inc.,” “Blue Cart Service, Inc.,” and “iMers, Inc.” These e-mails all used similar subjects, such as, “Thank you for using your free trial” or, “Your free trial period is almost over!”

Some phishing e-mails may not include any HPH language, but could still be directed towards individuals who work for healthcare-related organizations. The unintended victims in this instance may still have valuable HPH data unknowingly exfiltrated from their healthcare networks.

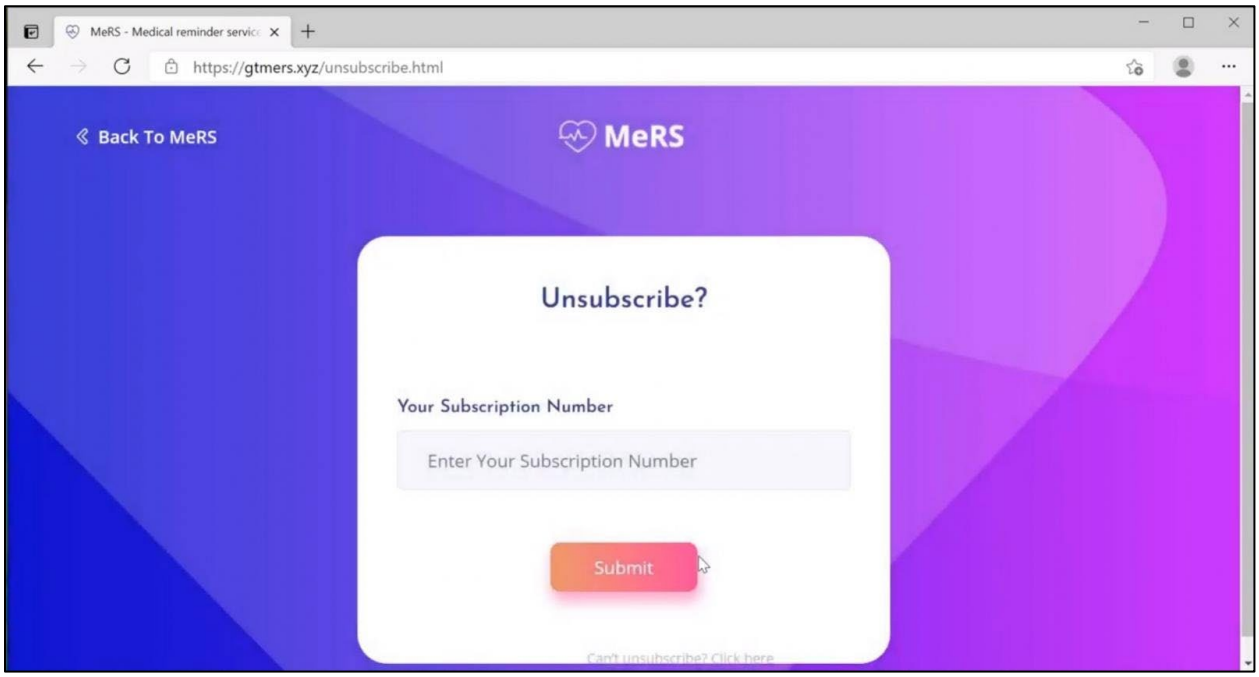


Figure 5: Sample Healthcare-Themed BazaCall Distribution Site. *(Source: BleepingComputer)*

Target Countries and Industries

As of 2022, the top target countries included the United States, Canada, China, India, Japan, Taiwan, the Phillipines, and the United Kingdom. As all three known threat actors – Silent Ransom, Quantum, and Roy/Zeon – are affiliated to previous Conti operators, this current list of target countries follows the defunct group and its offshoot groups’ geographic exclusionary pattern. Conti was known to exclude ex-Soviet or Commonwealth of Independent States (CIS) countries from being targeted in attacks.

While the HPH sector was known to be heavilty targeted, other industries known to have been affected by BazaCall campaigns included sporting teams, government and defense entities, IT solution providers, and technology and software companies.

HC3 Analyst Note
April 8, 2024 TLP:CLEAR Report: 202404081500

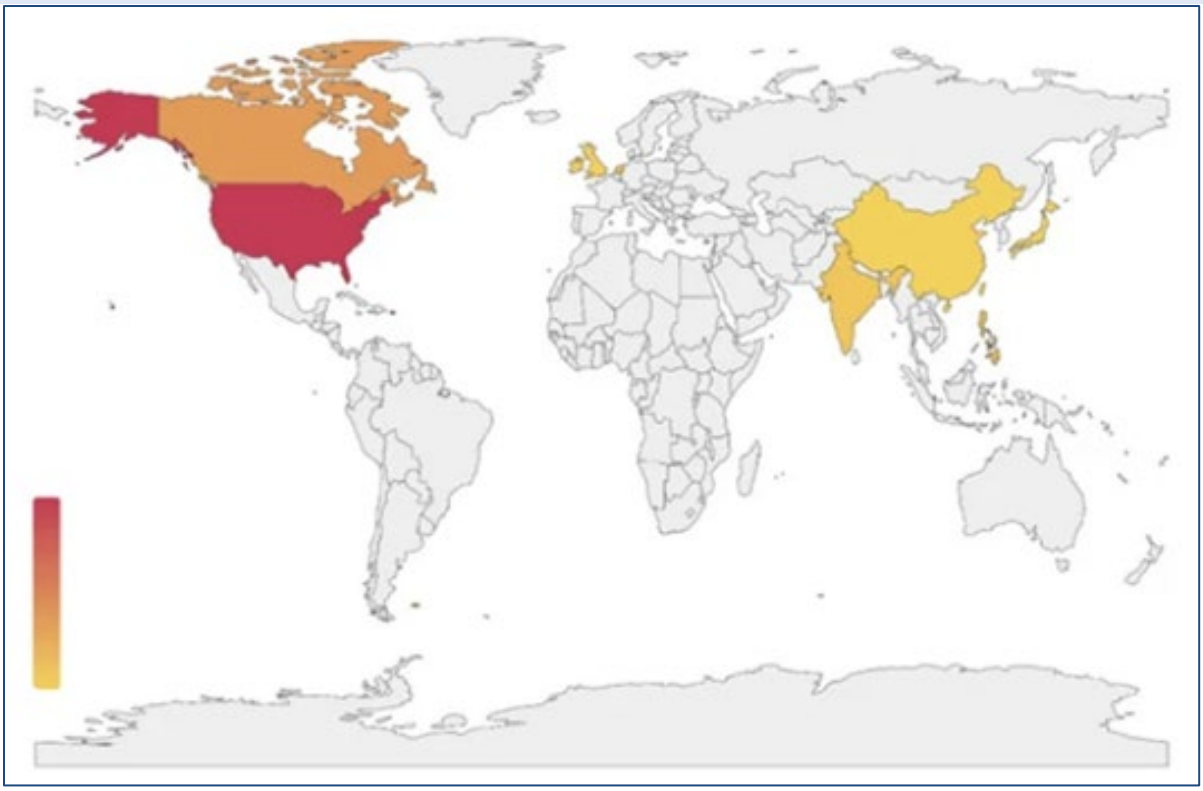


Figure 6: Map of Primary Target Countries by BazaCall Threat Actors in 2022. *(Source: The Hacker News)*

Indicators of Compromise

The following indicators have already been ingested into the Health-ISAC automated threat feed:

E-mail Addresses
info[@]icartservice.com
inform[@]icartservice.com
it[@]icartservice.com

Subjects
Do you want to extend your free period ##########?
Do you want to extend your free trial ##########?
Free period for ########## will come to the end end in 3 days
Free trial period for ########## ends in three days
Free trial period for ########## will end in 3 days
Your free period ########## is about to end!
Your free trial ########## is about to end!

Maldoc Download URLs
hxxps[:]//buyimers.us/unsubscribe.html
hxxps[:]//geticart.us/unsubscribe.html
hxxps[:]//getmers.us/unsubscribe.html

hxxps[:]//gobcs.us/unsubscribe.html
hxxps[:]//goimed.us/unsubscribe.html
Buyimers[.]us
Geticart[.]us
Getmers[.]us
Gobcs[.]us
Goimed[.]us

Maldoc (XLSB) File Hashes
09740a9d5d1b3d09d64d22d019567784
1974d98db0e8867165b008f7c46404a1
5a8f6aa70fae15ba88c0c159c30f923d
cdd3aacf99acd2a4e339914c480a6afd

Payload Download URLs
hxxp[:]//beauty1.xyz/campo/l/l1

Additional Payload File Hashes
1163[.]pk9
dd6cdec2609c165cc64b3bc22be5fe20
1163[.]ph5
99bfec83b97bd216e06117c6468b19db
1163[.]xlsb
99bfec83b97bd216e06117c6468b19db

MITRE ATT&CK Techniques

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objectives, and assess an organization's risk. While not exclusive, below are some sample MITRE ATT&CK techniques that have been used by threat actors relevant to this problem set:

Phishing	
ID: T1566	
Sub-Techniques	
T1566.001	Spear Phishing Attachment
T1566.002	Spear Phishing Link
T1566.002	Spear Phishing via Service
T1566.004	Spear Phishing Voice
Description	
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spear phishing. In spear phishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.	

HC3 Analyst Note
April 8, 2024 TLP:CLEAR Report: 202404081500

Adversaries may send victims e-mails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques, such as removing or manipulating e-mails or metadata/headers from compromised accounts being abused to send messages (e.g., E-mail Hiding Rules). Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human recipient, as well as automated security tools.

Victims may also receive phishing messages that instruct them to call a phone number, where they are directed to visit a malicious URL, download malware, or install adversary-accessible remote management tools onto their computer (i.e., User Execution).

Phishing for Information	
ID: T1598	
Sub-Techniques	
T1598.001	Spear Phishing Service
T1598.002	Spear Phishing Attachment
T1598.003	Spear Phishing Link
T1598.004	Spear Phishing Voice

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from general phishing in that the objective is gathering data from the victim rather than executing malicious code.

All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spear phishing. In spear phishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of e-mails, instant messages, or other electronic conversation means. Victims may also receive phishing messages that direct them to call a phone number, where the adversary attempts to collect confidential information.

Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human recipient as well as automated security tools.

Phishing for information may also involve evasive techniques, such as removing or manipulating e-mails or metadata/headers from compromised accounts being abused to send messages (e.g., E-mail Hiding Rules).

Phishing (Mobile Device)
ID: T1660

No Sub-Techniques
Description
Adversaries may send malicious content to users to gain access to their mobile devices. All forms of phishing are electronically delivered social engineering. Adversaries can conduct both non-targeted phishing, such as in mass malware spam campaigns, as well as more targeted phishing tailored for a specific individual, company, or industry, known as spear phishing. Phishing often involves social engineering techniques, such as posing as a trusted source, as well as evasion techniques, such as removing or manipulating e-mails or metadata/headers from compromised accounts being abused to send messages. Mobile phishing may take various forms. For example, adversaries may send e-mails containing malicious attachments or links, typically to deliver and then execute malicious code on victim devices. Phishing may also be conducted via third-party services, like social media platforms. Mobile devices are a particularly attractive target for adversaries executing phishing campaigns. Due to their smaller form factor than traditional desktop endpoints, users may not be able to notice minor differences between genuine and phishing websites. Further, mobile devices have additional sensors and radios that allow adversaries to execute phishing attempts over several different vectors, such as SMS messages, quick response (QR) codes, and phone calls.

Defense and Mitigations

In the absence of automatic threat detection systems, it is recommended that users find training to spot and report malicious e-mails. Regular training and simulated attacks can stop many threats and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Regardless of the social engineering vector used, the messaging and communications are malicious. This means users and organizations need to be vigilant across all communication channels; not just e-mails or text messages, but also traditional mail, phone calls, and internal systems as well.

In lieu of formal training, the following are additional recommendations users can take to help ensure they are not future victims:

- Verify that web links do not have misspellings or contain the wrong domain.
- Be suspicious of unsolicited phone calls, visits, or e-mail messages from unknown individuals claiming to be from a legitimate organization. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. If possible, try to verify the caller's identity directly with the company.
- If you receive a vishing call, document the phone number of the caller as well as the domain that the actor tried to send you to, and relay this information to law enforcement.
- Health-ISAC recommends appropriate user security awareness according to organizational policy, to include the possibility of applicable internal phishing exercises.

The Way Forward

While many cybersecurity threats rely on automated, drive-by tactics or develop advanced detection evasion methods, attackers continue to find success in social engineering and human interaction in attacks. The lack of typical malicious elements in BazaCall's e-mails, and the speed with which their operators can conduct an attack, exemplify the increasingly complex and evasive threats that organizatons

face today. Combined with a large populace that lacks training in phishing tactics, this distribution method will likely continue to be very effective.

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them, and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via e-mail and network access.
- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports

HC3: Alert – Conti Ransomware Amplify Alert (September 30, 2021)

HC3: Alert – Conti Ransomware (Update) (March 10, 2022)

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (May 9, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – Overview of Conti Ransomware) May 25, 2021

HC3: Analyst Note – Vishing Attacks on the Rise (August 19, 2022)

HC3: Threat Briefing – Conti Ransomware and the Health Sector (July 8, 2021)

HC3: Threat Briefing – Cybersecurity Incident Response Plans (October 12, 2023)

HC3: Threat Briefing – Data Exfiltration Trends in Healthcare (March 9, 2023)

HC3: Threat Briefing – The Impact of Social Engineering on Healthcare (August 18, 2022)

HC3: Threat Briefing – Multi-Factor Authentication & Smishing (August 10, 2023)

HC3: Threat Briefing – Strengthening Cyber Posture in the Health Sector (June 16, 2022)

HC3: White Paper – AI-Augmented Phishing and the Threat to the Health Sector (October 26, 2023)

HC3: White Paper – QR Code-Based Phishing (Quishing) as a Threat to the Health Sector (October 23, 2023)

References

Adams, Lawrence. "BazarCall malware uses malicious call centers to infect victims." BleepingComputer. March 31, 2021. https://www.bleepingcomputer.com/news/security/bazarcall-malware-uses-malicious-call-centers-to-infect-victims/

"BazaCall: Phony call centers lead to exfiltration and ransomware." Microsoft Security. July 29, 2021. https://www.microsoft.com/en-us/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/

"BazaCall Phishing Scammers Now Leveraging Google Forms for Deception." The Hacker News. December 13, 2023. https://thehackernews.com/2023/12/bazacall-phishing-scammers-now.html

Ilascu, Ionut. "Ransomware gangs move to 'callback' social engineering attacks." BleepingComputer. August 10, 2022. https://www.bleepingcomputer.com/news/security/ransomware-gangs-move-to-callback-social-engineering-attacks/

Lakshmanan, Ravie. "BazarCall Call Back Phishing Attacks Constantly Evolving Its Social Engineering Tactics." The Hacker News. October 11, 2022. https://thehackernews.com/2022/10/bazarcall-callback-phishing-attacks.html

Lakshmanan, Ravie. "Conti Cybercrime Cartel Using 'BazarCall' Phishing Attacks as Initial Attack Vector." The Hacker News. August 11, 2022. https://thehackernews.com/2022/08/conti-cybercrime-cartel-using-bazarcall.html

"Threat Bulletins: BazaCall Campaign Targets Healthcare Entities." Health-ISAC. July 30, 2021. https://www.aha.org/system/files/media/file/2021/07/h-isac-tlp-white-threat-bulletin-update-bazacall-campaign-targets-healthcare-entities-7-30-21.pdf

Vaas, Lisa. "BazaLoader Masquerades as Movie-Streaming Service." ThreatPost. May 26, 2021. https://threatpost.com/bazaloader-fake-movie-streaming-service/166489/

Vandenberg, Steve. "Microsoft Purview data security mitigations for BazaCall and other human-operated data exfiltration attacks." Microsoft Security. August 8, 2023. https://www.microsoft.com/en-us/security/blog/2023/08/08/microsoft-purview-data-security-mitigations-for-bazacall-and-other-human-operated-data-exfiltration-attacks/

HC3 Analyst Note
April 8, 2024 TLP:CLEAR Report: 202404081500

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback