KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Bizarre Social Engineering Tactics of BazarCall

Tracker ID: TN01013 **Date:** 17/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe, North America

Background

With the rise in cyberattacks, where individuals are becoming more aware of the common tactics used by adversaries, the evolution of BazarCall's social engineering strategies piques attention. In a recent campaign, BazarCall is shown constantly modifying and improving its social engineering strategies to deceive its innocent victims. The BazaCall callback phishing technique's developers have kept up with emerging social engineering techniques for spreading malware on targeted networks. The campaign eventually serves as a backdoor for financial fraud or the distribution of sophisticated payloads such as ransomware inside organizations. The United States, Canada, China, India, Japan, Taiwan, the Philippines, and the United Kingdom have lately been the primary targets of attack waves.

BazaCall, also known as BazarCall, rose to fame in 2020 for its novel technique of disseminating the malware known as BazarBackdoor or BazarLoader by manipulating potential victims into dialing a phone number provided in bogus email messages. These email baits attempt to create a sense of urgency by alerting recipients that a trial subscription for, like, an antivirus program is about to expire. The campaign was seen impersonating many brands like Geek Squad, Norton, McAfee, PayPal, Microsoft etc. Furthermore, the messages advise them to cancel the plan by contacting their support department to prevent being charged for the premium version of the software without their consent.

The assaults aim to gain remote access to the endpoint while pretending to cancel the subscription or to install security software to eliminate the infection from the computer, thus enabling further operations. Another approach employed by the operators is to pose as incident responders in campaigns with a PayPal theme to mislead the caller into believing that their accounts were accessed from eight or more devices located in various random locations around the world.

Regardless of the scenario, the victim is forced to click a specific URL, which leads to a specially crafted website that downloads and launches a malicious executable along with various other files. It also drops a genuine ScreenConnect remote desktop software. After successfully getting persistent access, the attacker would open bogus cancellation forms, deceiving users into giving money to the phisher by requesting personal information and bank account login details. Furthermore, this persistent access can be exploited to spy on the victim's activity, exfiltrate data, steal credentials, or infect the system with ransomware.

The victim also receives a fake refund success page, which convinces them that they have received their funds. As an additional strategy, the scammer sends an SMS to the victim with a phoney money received message to prevent the victim from suspecting any fraud. As the BazarCall campaign grew, it was discovered distributing more malware such as Trickbot, Gozi IFSB, IcedID, and others.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Bizarre Social Engineering Tactics of BazarCall

Tracker ID: TN01013 **Date:** 17/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe, North America

MITRE ATT&CK Tactics

Execution Defense Evasion, Collection, Credential Access, Discovery, Command and Control and Lateral Movement.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Refrain from opening untrusted links and email attachments without verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Ravie Lakshmanan, BazarCall Call Back Phishing Attacks Constantly Evolving Its Social Engineering Tactics, The Hacker News, 11th October 2022, External Link (thehackernews.com)
- Daksh Kapur, Evolution of BazarCall Social Engineering Tactics, Trellix, 06th October 2022, External Link (trellix.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Bizarre Social Engineering Tactics of BazarCall

Tracker ID: TN01013 **Date:** 17/Oct/2022 **Category:** Threat Actor **Industry:** All

Region: Asia, Europe, North America

Domain	Domain
hxxps://cslogin(.)xyz	hxxps://helpdeskcomputers(.)com(.)au
hxxps://remote(.)bankonitusa(.)com	hxxps://support(.)itsire(.)com
hxxp://nhelp(.)live	hxxps://hide03(.)xyz
hxxps://nhelp(.)live	hxxp://caresupport(.)cc
hxxps://help(.)applebyco(.)com	hxxps://caresupport(.)cc
hxxp://symetryk(.)com	hxxp://mwindows(.)live
hxxps://symetryk(.)com	hxxps://mwindows(.)live
hxxps://melogin(.)xyz	hxxp://teleassistenza(.)argosoft(.)it
hxxp://vfix(.)live	hxxps://login101(.)xyz
hxxps://vfix(.)live	hxxp://www(.)pifhelp(.)com
hxxp://caresupport(.)live	hxxps://asupport(.)to
hxxps://caresupport(.)live	hxxp://asupport(.)to
hxxp://www(.)asistpc(.)com	hxxps://helpservice(.)us
hxxp://213(.)246(.)45(.)32:8040	hxxps://clogin101(.)fun
hxxps://supportxxx(.)xyz	hxxp://csupportback(.)xyz
hxxps://supportlogin(.)xyz	hxxps://csupportback(.)xyz
hxxp://melogin(.)xyz	hxxps://sc2(.)in-sightsecurity(.)com
hxxp://carya(.)help	hxxp://ssiremote(.)com
hxxp://hide01(.)xyz	hxxps://ssiremote(.)com
hxxps://hide01(.)xyz	hxxp://pclogin(.)xyz
hxxp://deskhelp(.)me	hxxps://pclogin(.)xyz
hxxps://deskhelp(.)me	hxxps://loginuk(.)xyz
hxxps://mscare(.)live	hxxps://login02(.)xyz
hxxps://support(.)artemys(.)com	hxxp://qback(.)xyz
hxxp://supportlogin(.)xyz	hxxps://qback(.)xyz
hxxps://securemail(.)arescrow(.)com	hxxp://rlogin(.)xyz
hxxp://sc(.)admt(.)com:8040	hxxps://rlogin(.)xyz
hxxp://asupport(.)help	hxxps://support(.)dtslvinc(.)com
hxxps://asupport(.)help	hxxp://www(.)support247(.)pro
hxxps://onlogin01(.)xyz	hxxps://www(.)support247(.)pro
hxxps://support(.)marketsic(.)com	hxxps://123(.)serviciopr(.)com
hxxps://loginonly(.)xyz	hxxp://rsupport(.)me
hxxps://support(.)trade-center(.)net	hxxps://rsupport(.)me
hxxp://adasmarket(.)to	hxxps://control(.)ecomation(.)nl
hxxps://adasmarket(.)to	hxxps://support(.)fundremote(.)net
hxxp://deskhelpme(.)us	hxxps://www(.)303help(.)me
hxxps://deskhelpme(.)us	hxxps://my(.)aspire-it(.)net
hxxp://desksupport(.)us	hxxps://303help(.)me
hxxps://desksupport(.)us	hxxps://support(.)integrabeautyinc(.)com
hxxp://deskback(.)xyz	hxxps://pcsremotesupport(.)com
hxxps://deskback(.)xyz	hxxps://support247(.)pro
hxxps://www(.)stemsupport(.)me	hxxp://asupport(.)help/
hxxps://melogin101(.)fun	hxxps://hide17(.)xyz
hxxps://control(.)helpmis(.)com	