Phishing campaign threatens job security, drops Bazar and Buer Malware

By Elaine Dzuba

Published: 2020-11-09 · Archived: 2026-04-05 18:52:45 UTC

2020-11-09

7 min read

This blog originally appeared in November 2020 on the Area 1 Security website, and was issued in advance of Cloudflare's acquisition of Area 1 Security on April 1, 2022. Learn more.

“You’re fired……NOT!” An ongoing and rapidly evolving spear phishing campaign, hitting companies across industry verticals, is threatening targets with false claims of employment termination due to economic impacts from the global pandemic, among numerous other coercive tactics. The goal of the attacker is to intimidate employees into clicking on a link that will ultimately lead to Bazar or Buer malware infections by way of Trickbot.

Researchers at Zscaler ThreatLabZ noted this is the first time they have seen the two malware strains together. Additionally, they have associated this attack with the Trickbot gang, known to use a combination of different malware groups and bots to conduct attacks.

While Trickbot started out as a banking trojan, known for hijacking victims’ browser sessions once logged into their banking website, it has since been repeatedly repurposed for other objectives, including the ability to spread ransomware. This particularly maniacal and disruptive aspect of Trickbot functionality makes it a top contender for possible threats to the upcoming 2020 presidential election.

With ransomware as an option, Trickbot poses a significant threat to U.S. election infrastructure. The malware's operators have the ability to compromise a massive number of voting machines during critical times in vote counting, undermining trust in the result. That, or they may even be able to disrupt the voting process altogether by affecting entire voting locations, preventing large portions of the voter population from casting their ballots.

This could explain the recent wave of Trickbot takedown efforts. A report from KrebsonSecurity provided details of an operation that likely began on September 22nd and is conjectured to be a government counterstrike against the actors behind Trickbot. This activity, first identified by Intel471 and possibly conducted by the U.S. Cyber Command, attempted to disrupt Trickbot infrastructure by forcing the botnet's controllers to issue bogus configurations.

These configurations swapped real controller IP addresses for the localhost address (127.0.0.1), preventing bots from calling home to receive commands. Not long after the phony configurations were sent, all known controllers appeared to have stopped properly responding to bot requests, suggesting the overall activity was a concerted, intentional effort to disrupt this pervasive botnet's operations.

Another attempt was made on October 1st, presumably by U.S. Cyber Command, that similarly altered the controller IP addresses needed to receive commands. Compounding the effects of this effort, Microsoft also attempted disruptions of Trickbot infrastructure by obtaining a court order to disable the botnet's IP addresses, among other actions. Most recently, Microsoft issued an update that they successfully took down 62 of the 69 Trickbot servers around the world with the remaining being unorthodox IOT devices.

However, these attempts reportedly would only have a short-term effect on Trickbot controllers since its operators use decentralized infrastructure that communicates over Tor, with blockchain-based EmerDNS as a fallback that is resistant to takedowns. Additionally, Ars Technica reports that Trickbot controllers are beginning to host their malware on other e-criminals' servers.

Unsurprisingly, not long after the various Trickbot takedown operations occurred, Area 1 Security identified a prolific phishing campaign that intended to spread Bazar and Buer payloads via Trickbot. Worse yet, this newer stealthy malware in Trickbot gang's arsenal of tools can be used to deploy additional malware, including ransomware.

Area 1 Security researchers found evidence that the Bazar loader dropped in this campaign will not continue with the infection if the locale of the victim's device is in Russia, a common tactic seen with Trickbot. In fact, Cyber security researchers believe Trickbot is the handiwork of cybercriminals operating out of Russia. Since at least 2019, this group has been responsible for a surge in ransomware attacks targeting schools systems, local governments and even law enforcement agencies in the United States.

While these e-criminal groups have always been operating at some level in recent years, their activity has surged in the lead-up to the 2020 Presidential election. This suggests that entities involved in the U.S. election are prime targets for foreign adversaries, both nation-state and cybercriminal groups alike.

Lining up with the recent FBI/DNI press conference, Russian and Iranian state-sponsored groups are confirmed to have exfiltrated voter registration information. Additionally, these nations are behind separate email spoofing campaigns designed to undermine faith in the U.S. election.

At the moment, it is unclear if the phishing campaign that Area 1 Security identified is being carried out by any of these groups or if it is purposefully targeting election administrators. Regardless, state and local election administrators should be extra vigilant as they tend to be highly vulnerable to phishing attacks, as highlighted in a recent Area 1 Security phishing report.

Threatening Lures

This campaign employs a number of lures that threaten job security in order to intimidate targets into clicking on the provided URL. The phishing messages are very simple in their demand and appear to originate from persons of authority within the targeted company, as seen in Figure 1.

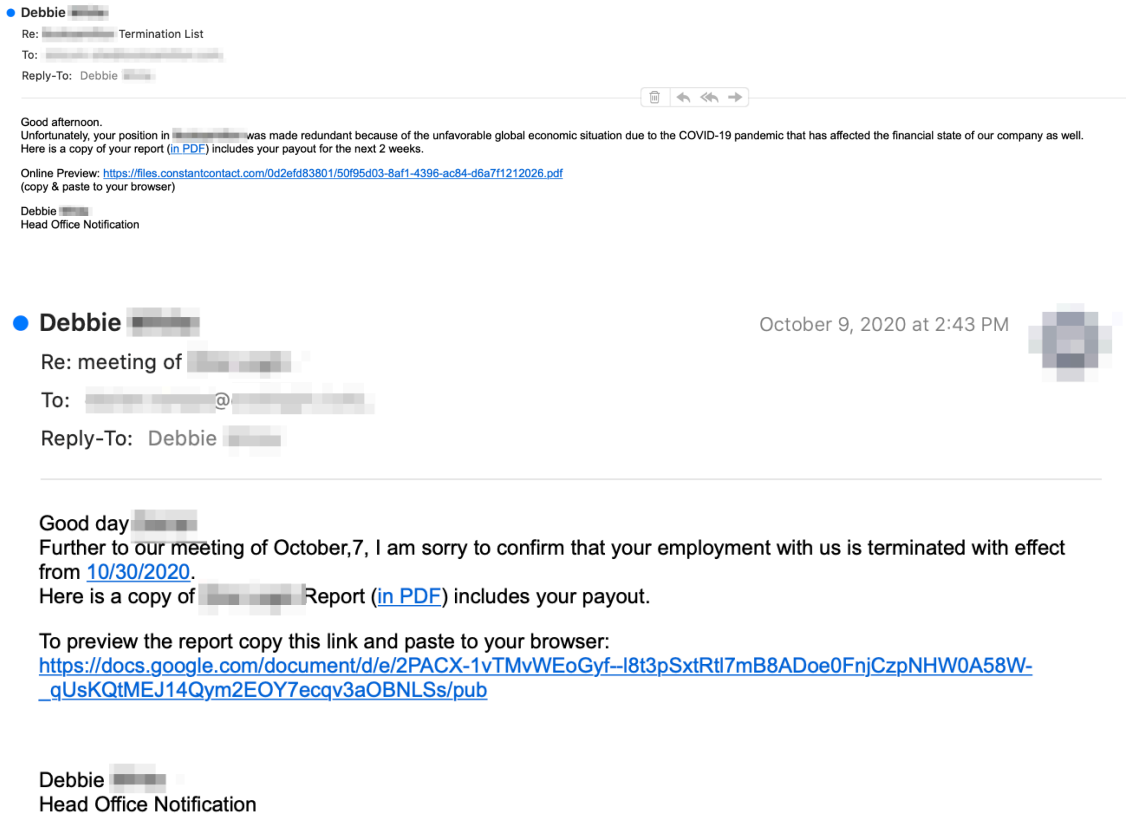

Figure 1. Phishing Messages That Threaten Job Security

The messages identified in this campaign are based on eliciting fear from the target audience, focusing on either employment termination or customer complaints. The current work-from-home operating model, and the resultant decrease in face-to-face contact, gives attackers the advantage by making email delivery of these types of “employment notifications” all the more believable.

Targets of this campaign could potentially believe that the post COVID shake up in their organizations is the reason they’re being let go. With many businesses closing down unusable office space, combined with an economic recession, there is enough plausibility for this wide-ranging attack to fool employees into believing that their position may be part of the now all-too-common budget cuts.

It's possible this Bazar and Buer campaign is part of the Trickbot operations that Microsoft and other partners are trying to defeat. If so, the activity Area 1 Security observed only further proves just how difficult it can be to

counteract these complex operations. A litany of unique and ever-changing email accounts and IP addresses are at the threat actor's disposal. Despite the previously mentioned efforts to neutralize Trickbot controllers, the infrastructure used to support this particular campaign (if associated in any way) was hardly affected, where the attacker seems to have promptly resumed operations.

While disruption operations may have worked a decade ago, the Trickbot gang and other groups that rely on their Malware-as-a-Service (MaaS) offering are equipped with the necessary skills to continue their attacks without a hitch. Current botnets have all the professionalism of any IT company. They're able to manage disruptions and bring back services with continuity planning, backups, automated deployment, and a dedicated workforce.

The campaign noted above centered on termination-related documents available at a provided URL. When clicked, the link directs the victim's browser to either Google Docs or Constant Contact. By not attaching the malware as a file to the email, the attacker is able to bypass file scanning detections. Moreover, the use of common cloud-based hosting services allows the attacker to circumvent URL scanning techniques, as well as enables them to easily create new malicious links in the event that their URLs are identified as phishing pages.

The Google Docs or Constant Contact link in the email leads to a decoy preview page, as shown in Figure 2, that prompts the victim to open a list of terminated employees. The decoy also cleverly displays the often seen "If download does not start, click here". This link is where the malware is actually being hosted.

Figure 2. Google Doc Decoy Preview Page with Redirect Link

Analysis of Malware

As seen in the figure below, after clicking on the link found in the online document, the victim is presented with a dialog box to run the file. The file is actually a malicious PE32+ executable that is designed to run on all Windows systems.

Figure 3. Gaining Run Permission

After clicking “Run”, a series of events will take place on the victim’s device that will ultimately lead to installation of the Bazar backdoor or Buer loader.

First, the PE32+ executable noted above will decrypt the payload using an RC4 cipher, a portion of which is provided in Figure 4 below. The payload happens to be none other than Trickbot, and a different RC4 key is used for each iteration of the malware.

```
lea     rcx, key        ; "ecW4N?iLE!Rz!#@MW)K+K!+uz)cMAn*S$g)W&Aa"...
call    _Z11prepare_keyPhiP7rc4_key ; prepare_key(uchar *,int,rc4_key *)
mov     edx, dword ptr [rbp+Size]
lea     rcx, [rbp+var_90]
mov     rax, [rbp+Dst]
mov     r8, rcx
mov     rcx, rax
call    _Z3rc4PhiP7rc4_key ; rc4(uchar *,int,rc4_key *)
mov     rax, [rbp+Dst]
mov     [rbp+var_70], rax
mov     rax, [rbp+var_70]
call    rax
```

Figure 4. RC4 decryption of Trickbot Payload

As detailed in Figure 5, Area 1 Security researchers identified the string “dave” at the end of the Trickbot payload in memory, which is consistent with prior reporting on techniques employed by Emotet and Trickbot malware developers. This string reveals the attacker’s use of a custom packer to compress and encrypt the file, making it difficult for malware analysts to reverse engineer the payload.

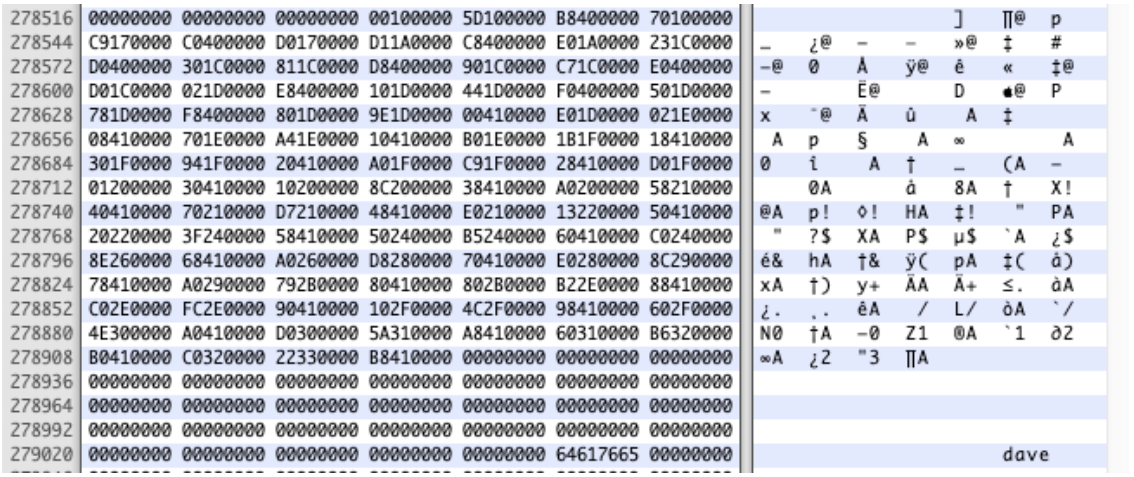

Figure 5. “Dave” signature

Despite this anti-reversing technique, Area 1 Security discovered the Trickbot payload attempts to further infect the victim device by decrypting and running the BazarLoader. Loaders are an essential function that allow attackers to gain a foothold in a network and enable subsequent, more persistent infection via their command and control servers. This tactic opts for stealth by initially loading as little functionality as necessary.

In this case, the BazarLoader in turn attempts to download the Bazar backdoor via a blockchain dns lookup table. This is a great tactic for attackers as it circumvents the need for traditional ISPs. Similar to bitcoin, Top Level Domains (TLDs) like .bit, .bazar, and .coin are not owned by a single authority but instead shared over peer-to-peer networks. This offers users the ability to bypass censorship and other government restrictions, but also provides a platform for attackers to conduct illicit activities that are safe from countermeasures.

As shown in Figure 6, to download the backdoor, the loader loops through eight unique IP addresses and five domains under the EmerDNS .bazar TLD.

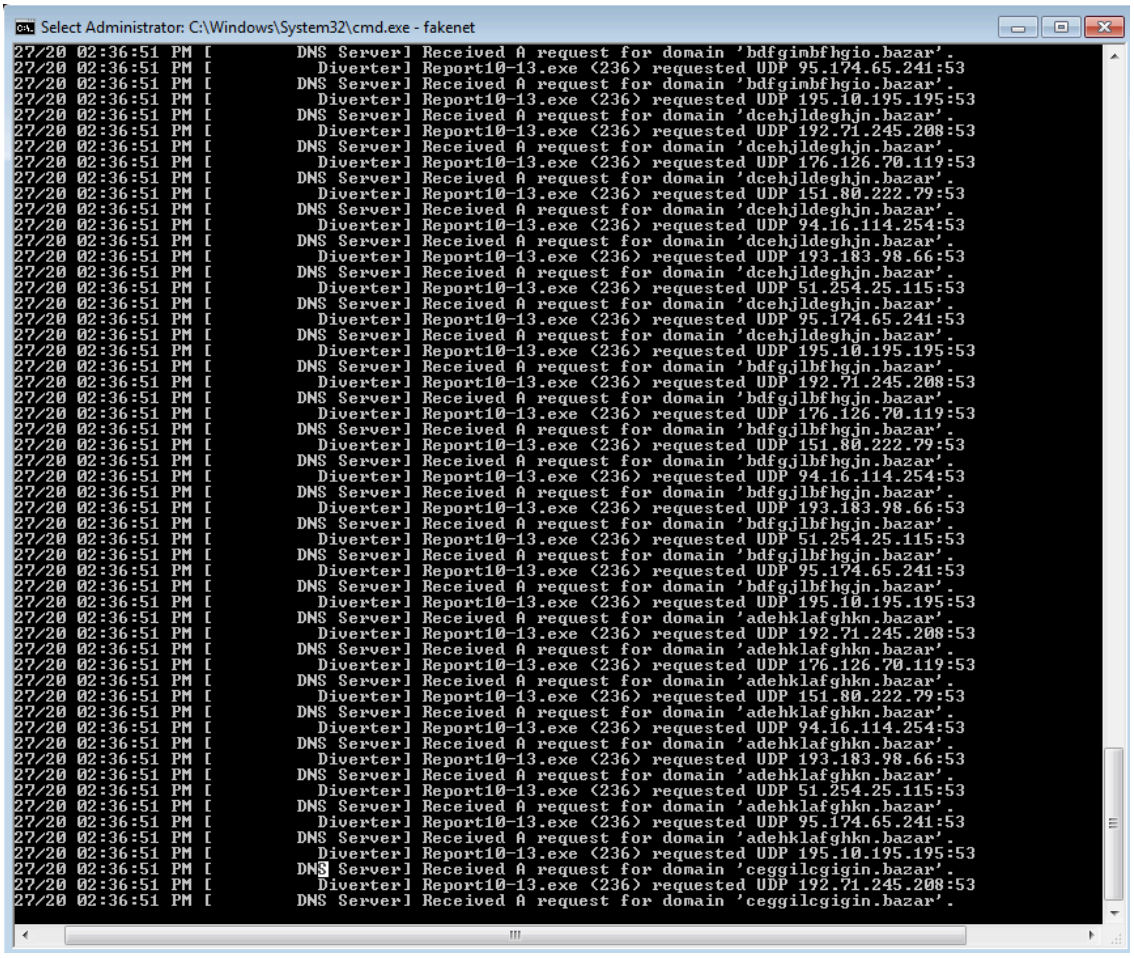

Figure 6. Outbound Connections to Download the Bazar Backdoor

The second level domains are comprised of 12 alphabetical characters that are generated using a specific domain generation algorithm. The malware runs through the list of generated .bazar domains to find one that is still actively hosting the backdoor.

Once the backdoor is downloaded and successfully run, that attacker can carry out any number of devious acts, including remotely executing commands, exfiltrating sensitive data, and deploying other payloads. These additional payloads range anywhere from post-exploitation frameworks like CobaltStrike to ransomware like Ryuk.

In fact, Trickbot is known to deliver Ryuk ransomware to devices via BazarLoader. In one instance, after the initial Bazar infection, attackers exploited a recently disclosed vulnerability to escalate privileges and gain domain-wide ransomware infection just 5 hours after sending their phishing message. This is unfortunately just one of many possible outcomes that can result from successful infection via the phishing campaign Area 1 Security has observed.

Recommendations

By leveraging a number of stealthy techniques, the threat actors behind this campaign have been able to easily evade legacy vendors and cloud email providers. Linking to legitimate, cloud-based sites within the phishing

messages, combined with the use of takedown- and sinkhole-resistant EmerDNS TLDs, makes this a particularly difficult campaign to detect.

Area 1 Security‘s advanced Machine Learning and Artificial Intelligence technology allow our algorithms to uncover the clever tactics seen in this campaign, enabling us to block the messages in real time versus waiting days or weeks for signature updates. Our time-zero detections lead the industry with reliable verdicts that stop phishing attempts at delivery time. This means malware like Trickbot, the Bazar backdoor, and follow-on infection with ransomware, never have the opportunity to make their way onto our customers’ devices. Our solution has many advantages over post-delivery retraction in that the user is never exposed to the attack.

Indicators of Compromise

Phishing Email Subject Lines:

Re: Termination List

RE: termination,

Re: my visit and call

Re: meeting of

RE: office

RE: office,

Malicious PE32+ Executable Linked to in Decoy Document:

Sha1: 895d84fc6015a9ad8d1507a99fb44350fb462c79

Sha256: a3b2528b5e31ab1b82e68247a90ddce9a1237b2994ec739beb096f71d58e3d5b

Md5: dbdb5ddd07075b5b607460ea441cea19

Sites Hosting Malicious PE32+ Executable:

hxxps://tees321[.]com/Document3-90[.]exe

hxxps://centraldispatchinc[.]com/Report10-13[.]exe

hxxps://www[.]4rentorlando[.]com/Text_Report[.]exe

Malicious Links in Phishing Messages:

hxxps://files.constantcontact.com/0d2efd83801/50f95d03-8af1-4396-ac84-d6a7f1212026.pdf

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQzFpGbLRNSIpbklM51_9P78DJbhxmMLeMzQUJxX9roupKMn3xYX1ZBEjP2Jo5_CHbzoqIdVnwPeazU/pub

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRhLU8Ar86crHTwsP7rSyStmTABnsPtQ4q3Mic9UIZN-hz06cO8fuzsiiEus9seLQHDU4T51YGcejNU/pub

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vTVCHKzmdSD2wX03GTnyBToo4xvldfGqtFWZiz5bT5cTRozW4Xk5H6GER0GmscSPqnpyFtokphDl-_U/pub

hxxps://files[.]constantcontact[.]com/5e536f60101/8c5d270a-897a-4ac8-845a-86c920bf229c[.]pdf

hxxps://files[.]constantcontact[.]com/defde16c001/0aa90d3a-932f-4343-8661-22e4f6488705[.]pdf

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vSlUktRROV3hU60c_n8LWFpOQBdyJj-N10g4tn14hBfmdaiRGKL9rc4vnTRYdLErwU0AHt7WwbzwU9q/pub

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRFLfuWRihaQHjGEPs8-Dm7Y3VxEFRpiUJuJmD9Vm6y3xVSSG9Vc3XxRnbyHQzIoWQ_5REbdDbkOq0s/pub

Outbound BazarLoader DNS Requests (Port 53):

95[.]174[.]65[.]241:53

195[.]16[.]195[.]195:53

192[.]71[.]245[.]208:53

176[.]126[.]70[.]119:53

151[.]80[.]222[.]79:53

94[.]16[.]114[.]254:53

193[.]183[.]98[.]66:53

51[.]254[.]25[.]115:53

Blockchain Domains:

bdfgimbfhgio[.]bazar

dcehjldeghjn[.]bazar

bdfgjlbfhgjn[.]bazar

adehklafghkn[.]bazar

ceggilcgigin[.]bazar

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Email SecurityCloud Email SecurityPhishingMicrosoft
