BazarLoader Campaign with Fake Termination Emails

hornetsecurity.com/en/threat-research/bazarloader-campaign-with-fake-termination-emails/

Security Lab October 13, 2020

Summary

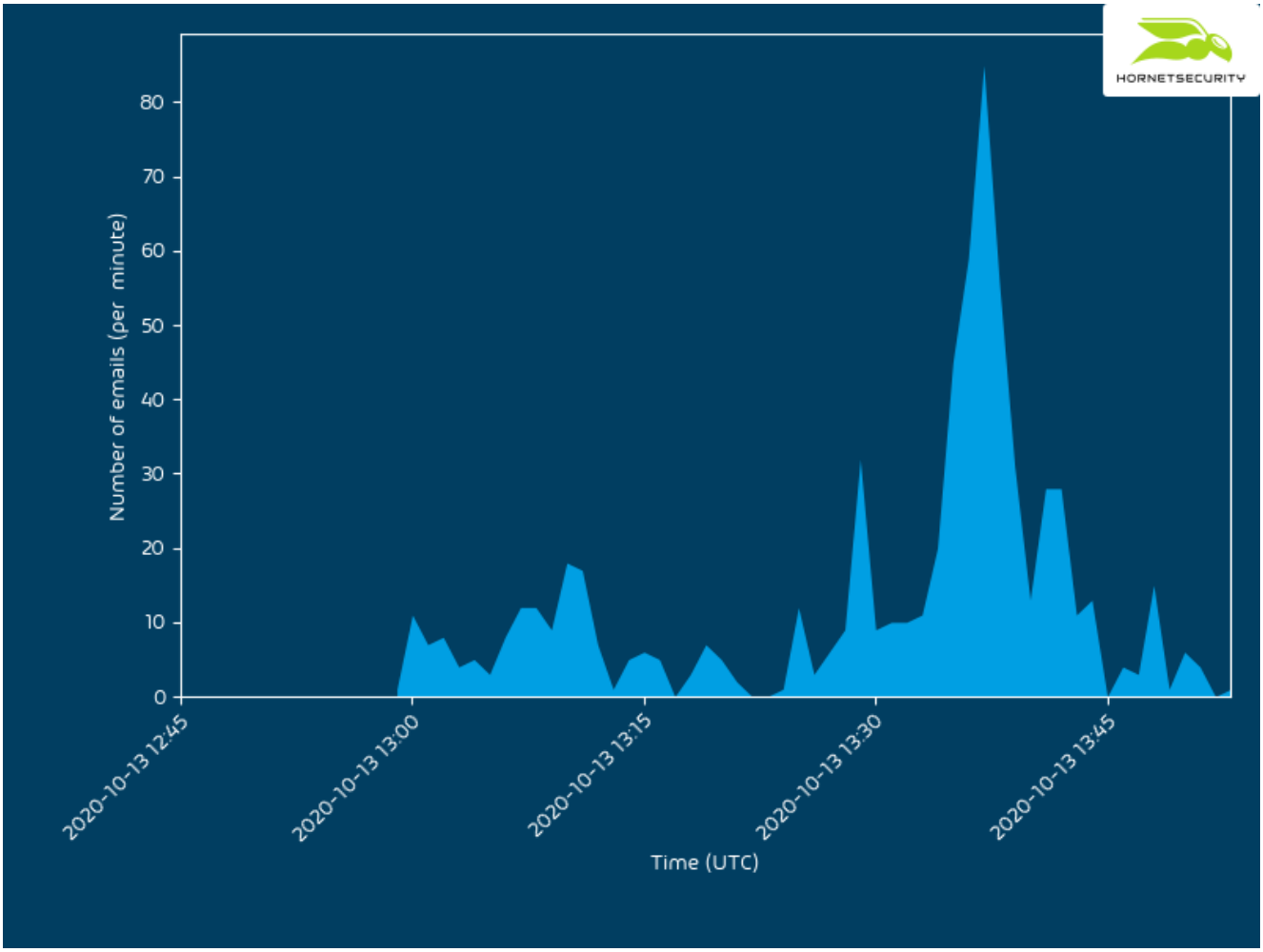
Hornetsecurity has observed a malicious email campaign distributing the BazarLoader using termination as a lure. The campaign uses a link to Google Docs from where the BazarLoader malware executable is downloaded.

Background

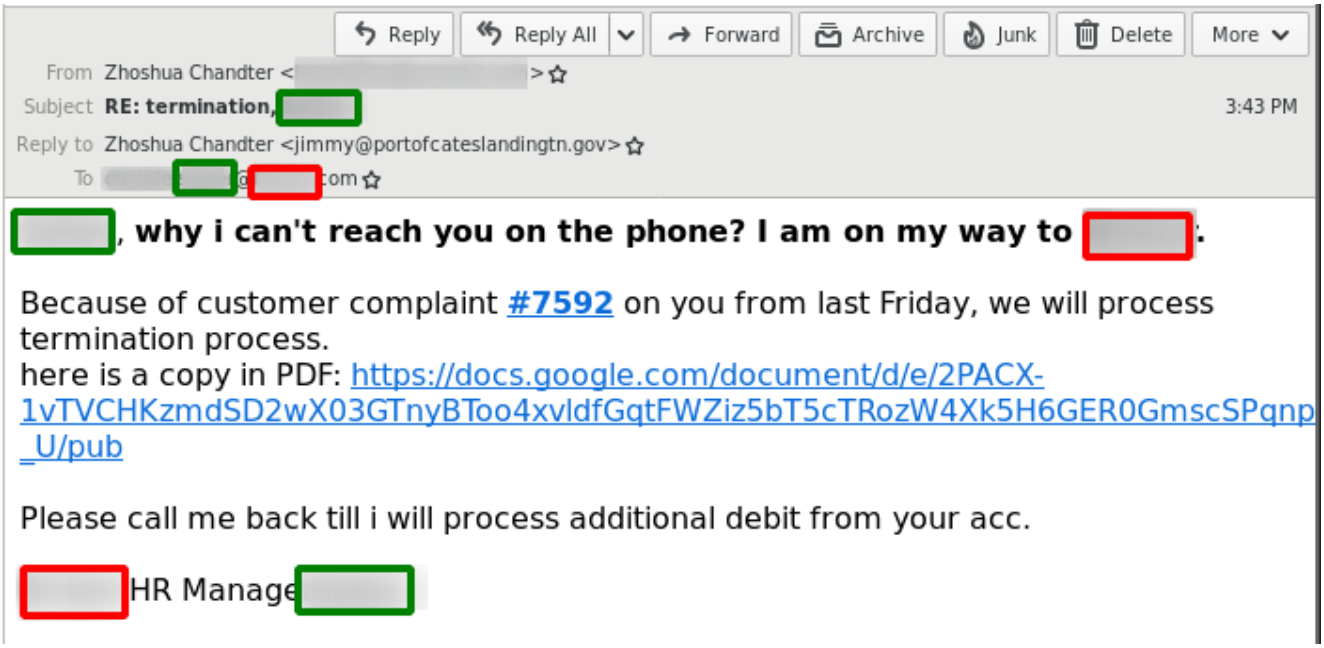
BazarLoader is a new malware loader attributed to a threat actor with a close relation to the TrickBot malware. The loader is also aptly named KEGTAP, as in device used to open a beer keg[3], because it is used to “open” the network of victims for follow up malware in order to move laterally on the network and eventually deploy ransomware.

Technical Analysis

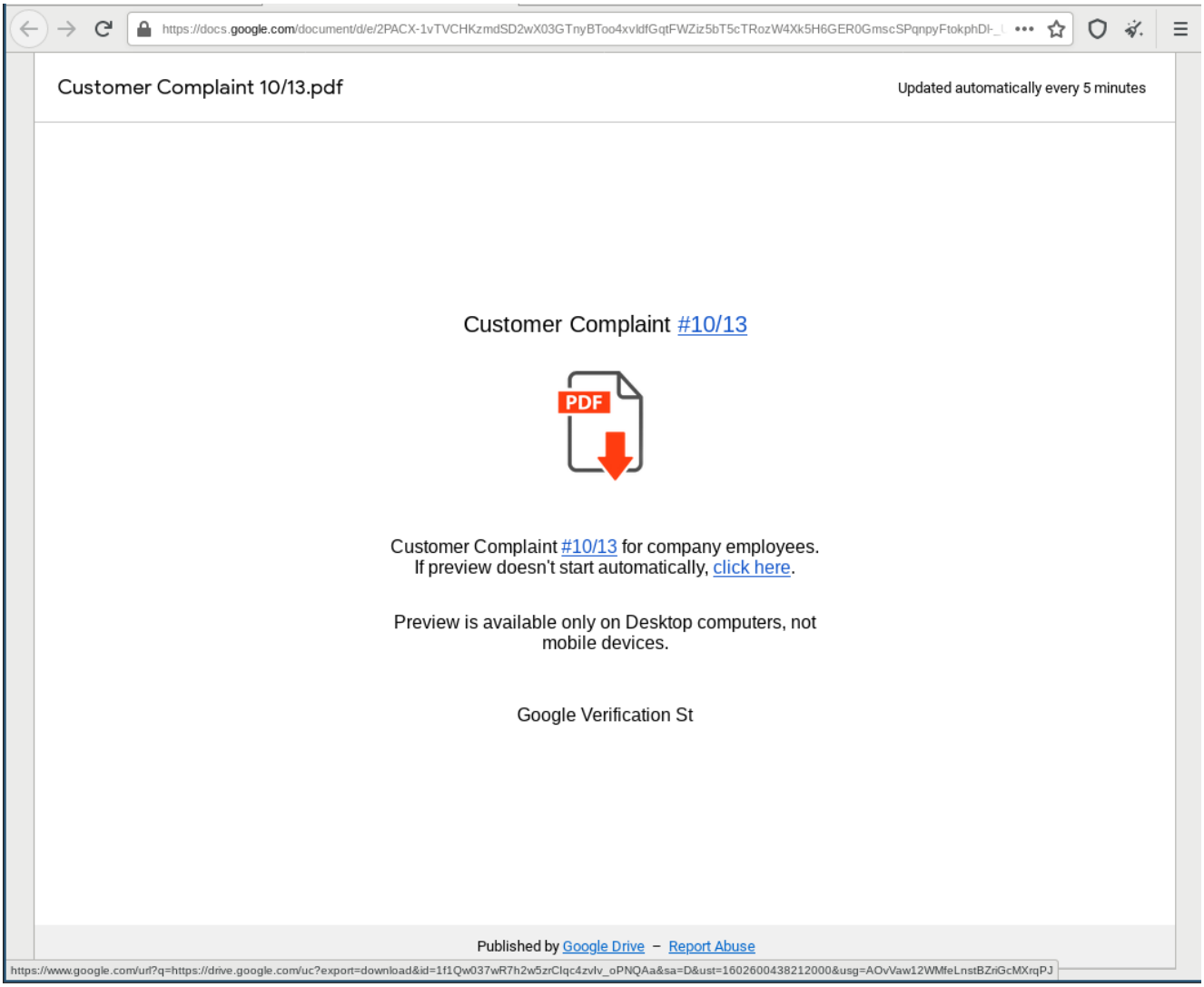
On 2020-10-13 at exactly 13:00 UTC Hornetsecurity registered the first emails of the new BazarLoader campaign:



The emails use a termination lure:



The URL in the email is a legitimate Google Doc URL:



From their all links lead to the BazarLoader executable (`Report10-13.exe`).

When executed, BazarLoader will use OpenNIC Public DNS Servers to resolve a `.bazar` domain generated via domain generation algorithm (DGA). The `.bazar` domain is not a regular TLD but rather an alternative DNS TLD of the decentralized EmerDNS blockchain DNS system.

No.	Time	Source	Destination	Protoc	Lengt	Info
5629	152.185500096	172.16.42.101	95.174.65.241	DNS	78	Standard query 0x0003 A bfehkmbmghko.bazar
5630	152.186544312	172.16.42.101	195.10.195.195	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5638	152.694876120	172.16.42.101	192.71.245.208	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5639	152.695907101	172.16.42.101	176.126.70.119	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5640	152.696533559	172.16.42.101	151.80.222.79	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5641	152.697186411	172.16.42.101	94.16.114.254	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5642	152.697814931	172.16.42.101	193.183.98.66	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5643	152.698310207	172.16.42.101	51.254.25.115	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5644	152.698975782	172.16.42.101	95.174.65.241	DNS	78	Standard query 0x0004 A bcggilbjigin.bazar
5645	152.700123229	172.16.42.101	195.10.195.195	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5671	153.209139232	172.16.42.101	192.71.245.208	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5686	153.710221665	172.16.42.101	176.126.70.119	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5688	154.226365486	172.16.42.101	151.80.222.79	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5752	154.728070214	172.16.42.101	94.16.114.254	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5754	155.241106615	172.16.42.101	193.183.98.66	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5755	155.241464038	172.16.42.101	51.254.25.115	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5756	155.241918790	172.16.42.101	95.174.65.241	DNS	78	Standard query 0x0005 A bcgikkbjiikm.bazar
5757	155.242323641	172.16.42.101	195.10.195.195	DNS	78	Standard query 0x0006 A adgiklakiikn.bazar
5762	155.758709559	172.16.42.101	192.71.245.208	DNS	78	Standard query 0x0006 A adgiklakiikn.bazar
5764	156.273486009	172.16.42.101	176.126.70.119	DNS	78	Standard query 0x0006 A adgiklakiikn.bazar

Then the BazarLoader will download and install the BazarBackdoor[1]. This backdoor will be used to move laterally in the victim's network in order to take over the domain controller. Eventually the intrusion is monetized by deploying the Ryuk[2] ransomware.

Conclusion and Countermeasure

Because the payload download is hosted on the legitimate Google Docs site victims are more likely to click the link in the email then they would an obscure URL they are unfamiliar with. BazarLoader's use of the EmerDNS blockchain DNS system makes it immune to current efforts by various security vendors to disrupt the operations of TrickBot.

Hornetsecurity's Spam Filter Service and Malware Protection, already detects and quarantines the outlined threat emails.

References

Indicators of Compromise (IOCs)

Hashes

MD5	Filename	Description
`9cd1f319f58c3979399c1779d5a34bc2`	`Report10-13.exe`	BazarLoader

IPs

OpenNIC Public Servers used by the analyzed BazarLoader version:

- `195.10.195.195` (53/udp)
- `192.71.245.208` (53/udp)
- `172.126.70.119` (53/udp)
- `151.80.222.79` (53/udp)
- `94.16.114.254` (53/udp)
- `193.183.98.66` (53/udp)
- `51.254.25.115` (53/udp)
- `95.174.65.241` (53/udp)

URLs

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