A Baza Valentine’s Day

proofpoint.com/us/blog/threat-insight/baza-valentines-day

February 11, 2021

Blog
Threat Insight
A Baza Valentine’s Day

February 11, 2021 Proofpoint Threat Research Team

In 2020, Proofpoint observed an increase in BazaLoader campaign volume peaking in October. During that time, we observed specific campaigns correlated to public reports of affiliate campaigns delivering BazaLoader and associated with Ryuk ransomware infections. Notably, in January 2021, Proofpoint researchers observed a few of BazaLoader campaigns leveraging Valentine's Day themes such as flowers and lingerie. The attack chains required an unusual amount of human interaction before a payload was delivered. While we track a fair amount of BazaLoader delivered by TA800 and TA572, these campaigns are not associated with either TA800 or TA572 and are likely leveraged by other affiliates.

BazaLoader Origin

BazaLoader is a downloader written in C++ whose primary function is to download and execute additional modules. It was first observed in the wild in April 2020 and since has steadily been adopted by more actors. Proofpoint has observed at least six variants of Bazaloader signaling active and continued development. One of the earliest BazaLoader variants Proofpoint researchers identified used ".bazar" top-level domains for command-and-control communication. The ".bazar" TLDs are associated with cryptocurrency DNS named Emercoin using Blockchain services reported in early April 2020. Today, we do not see the same association to cryptocurrency infrastructure, but it is relevant to its provenance.

Valentine's Day

Proofpoint researchers have spotted multiple BazaLoader campaigns in January and February 2021 involving the tactic of heavily relying on human interaction with different sites, PDF attachments, and email lures. There were a range of lure and subject topics, including compact storage devices, office supplies, pharmaceutical supplies, and sports nutrition, but what stuck out were campaigns that were timely and relevant to the upcoming Valentine's Day holiday. The campaigns were spread across a diverse set of companies and sectors.

Valentine's Day, while not abused to the level of other holidays, presents an opportunity for a variety of actors. The FBI Boston field office has posted public warnings of romance scams. While this is not a romance scam, it is an example of social engineering well-timed with the Valentine's Day holiday.

Infection Chain

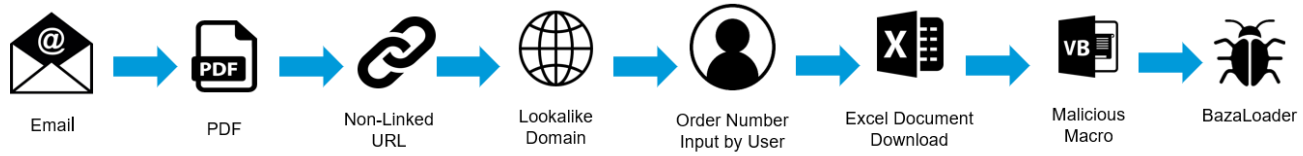


Figure 1: Infection Chain

The infection chain is consistent in the latest campaigns. The websites the user would browse to are fake, but the actors took care to have the physical addresses in the below images match a near-legitimate location. For example, Ajour Lingerie is not located at 1133 50th St, Brooklyn, NY 11219, but this address is in physical proximity to a legitimate website and physical business called the Lingerie Shop.

Figure 2: physical address to digital website

Lingerie at Ajour

This campaign delivered PDF attachments that references a specific customer order number and associated purchased items which entices the recipient to go to the Ajour Lingerie website. If the user visits the website and navigates to the "Contact Us" page, they are then given the option to enter the order number in the order ID. If entered, the contact page then redirects the user to the landing page that links to and explains how to open the Excel sheet. The Excel sheet contains macros that, if enabled by the user, will download BazaLoader.

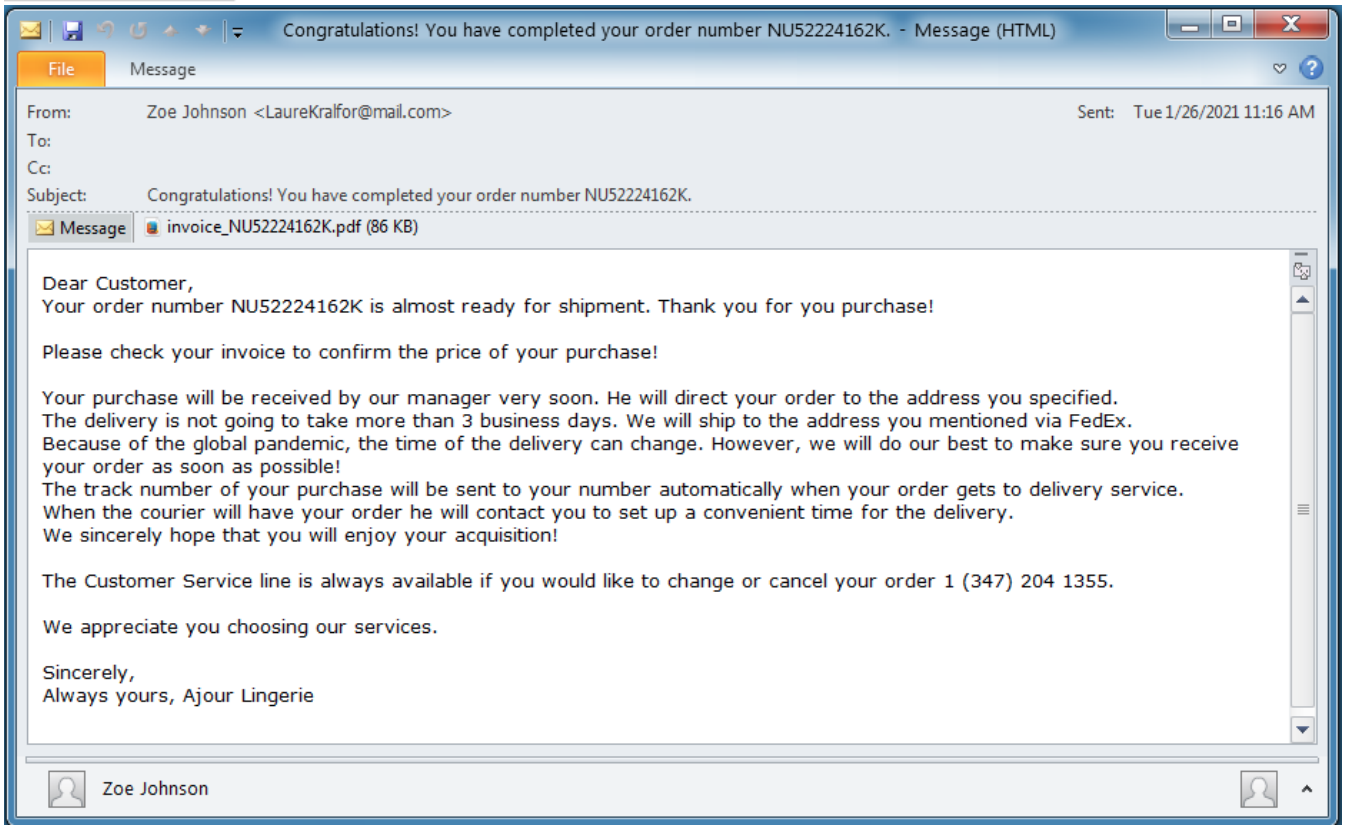


Figure 3: Email Lure

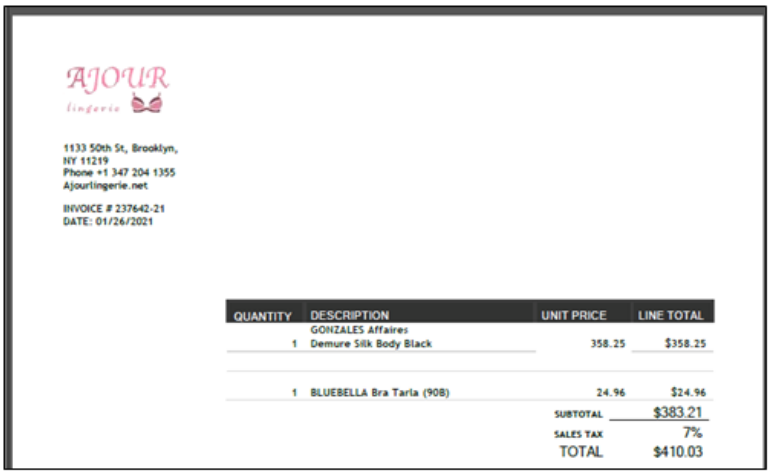


Figure 4: Ajour Lingerie

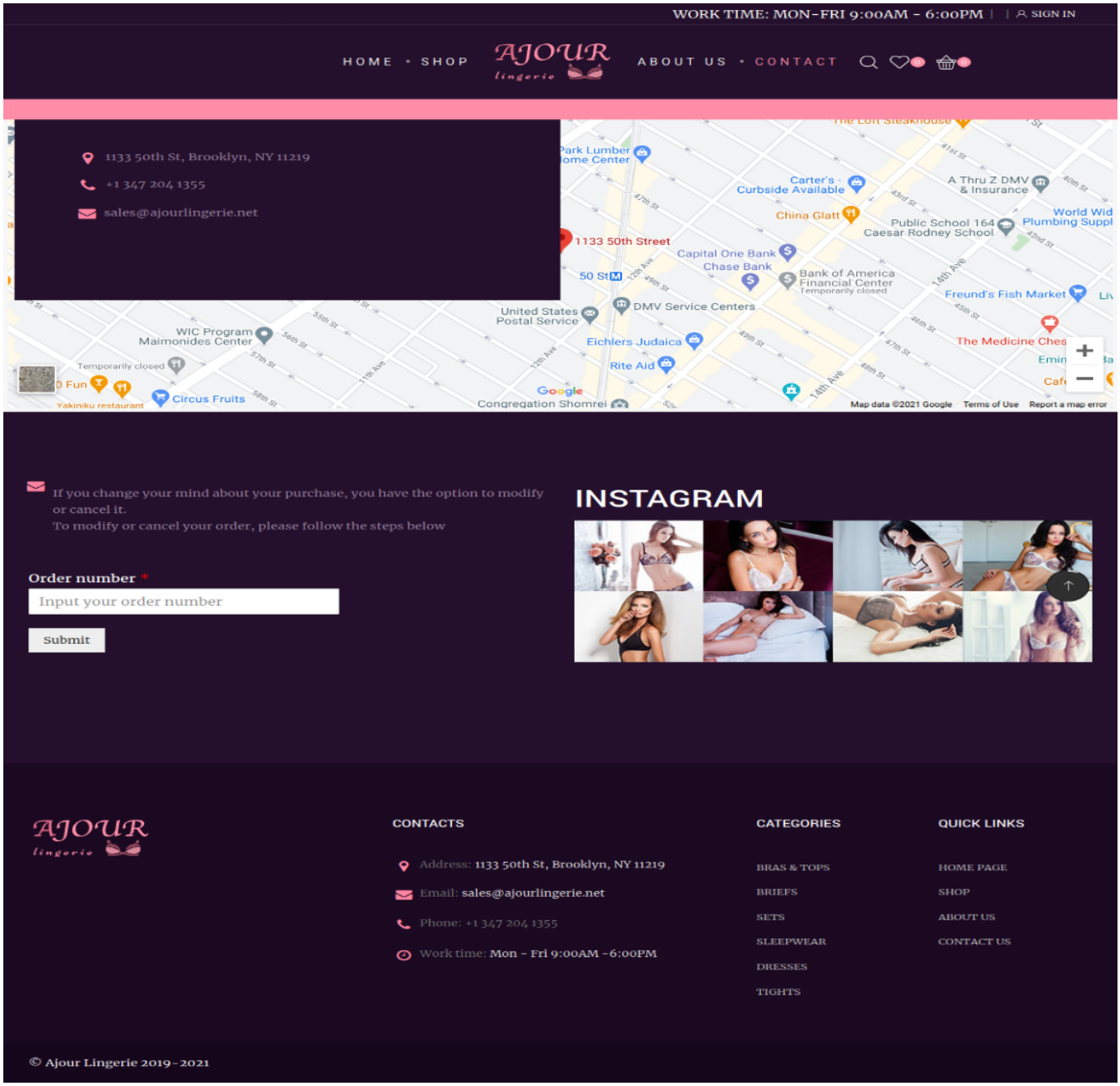


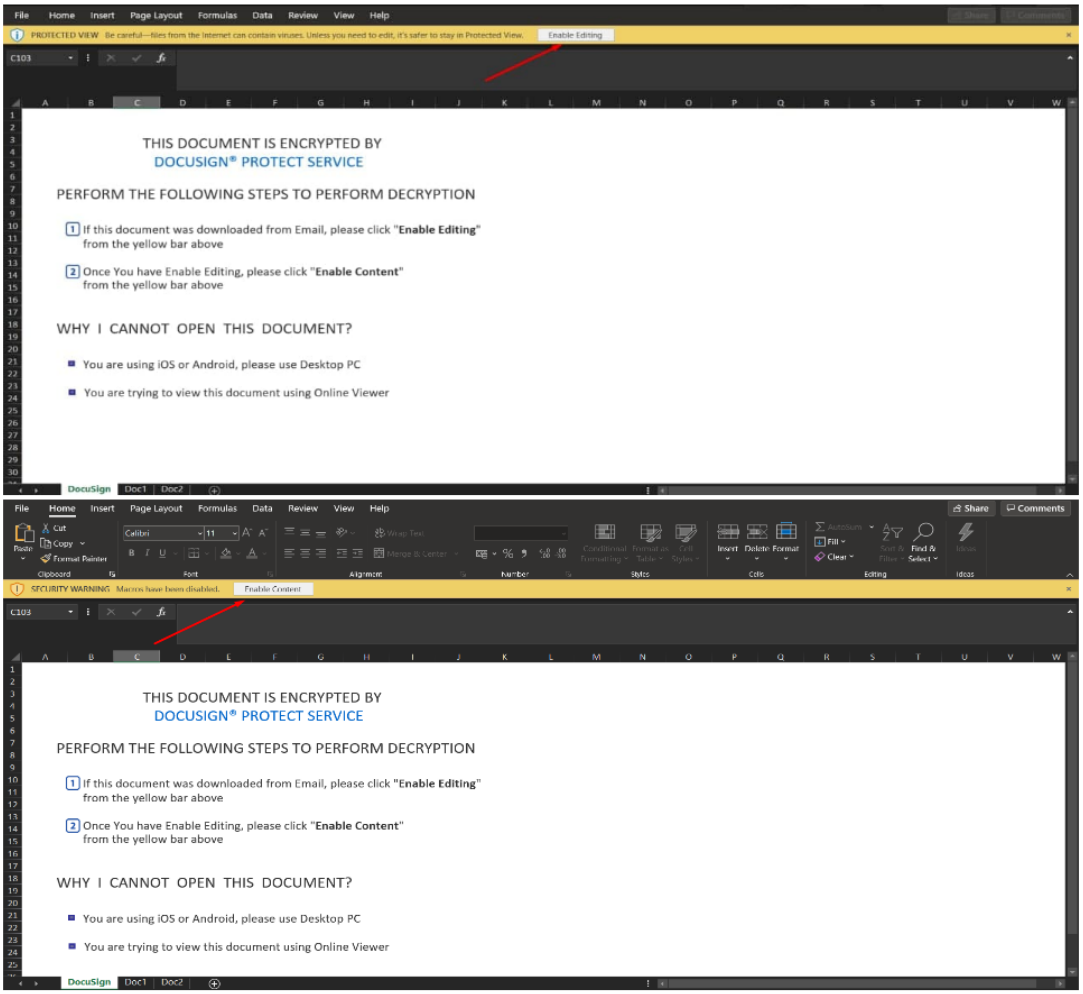
Figure 5: Landing Page

AJOUR
lingerie

Order status: processed

Your order is being processed at 01.26.2021. In case you want to modify or cancel it, please follow next step

Open the document, "Enable Editing" and "Enable Content" to be able to fill out the form.



Only for Google Chrome users

Help

The form could be downloaded here:

Request Form

Send the filled out form to this email

Figure 6: Enable Content to deliver BazaLoader

Flowers at Rose World

This campaign is nearly identical—enticing users to check an order number. The campaign delivered PDF attachments with references to purchases at the Rose World website. If the user visits the website, navigates to "Contact Us", and enters the order number in the order ID, the site will redirect the user to a landing page. This landing page links to and explains how to

open the Excel sheet. The Excel sheet contains macros that, if enabled, will download BazaLoader.

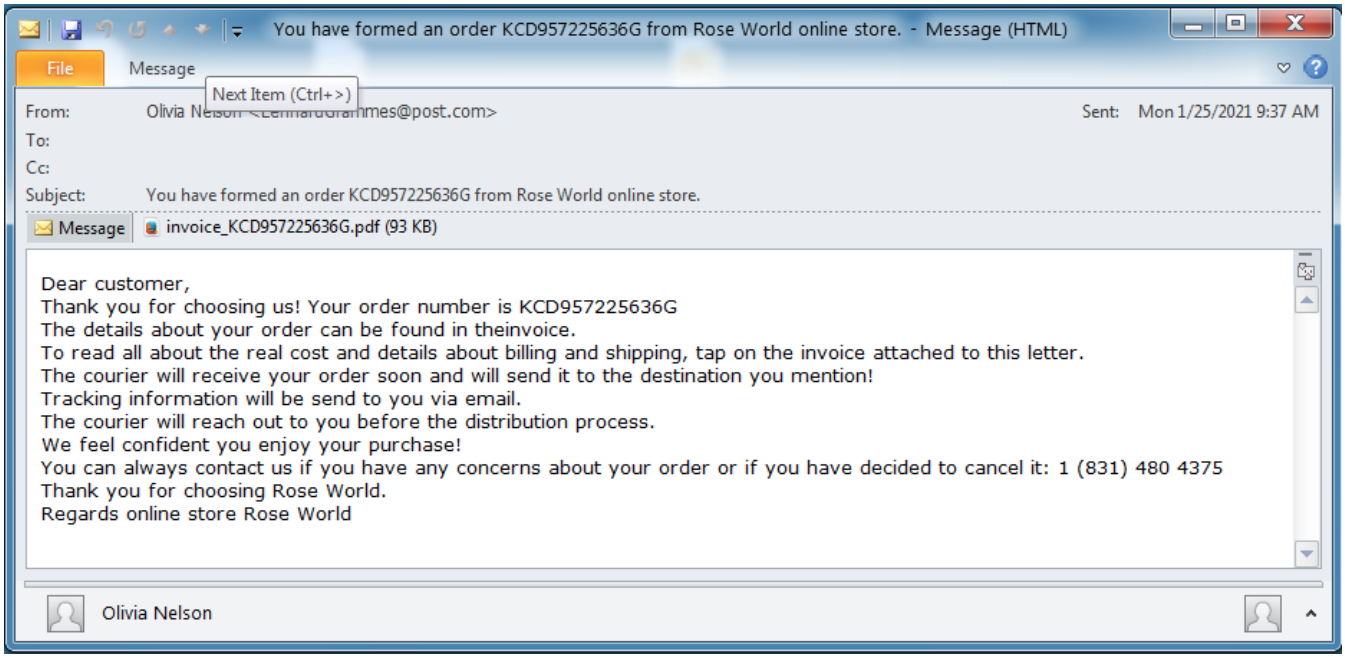


Figure 7: Rose World Customer Order Email

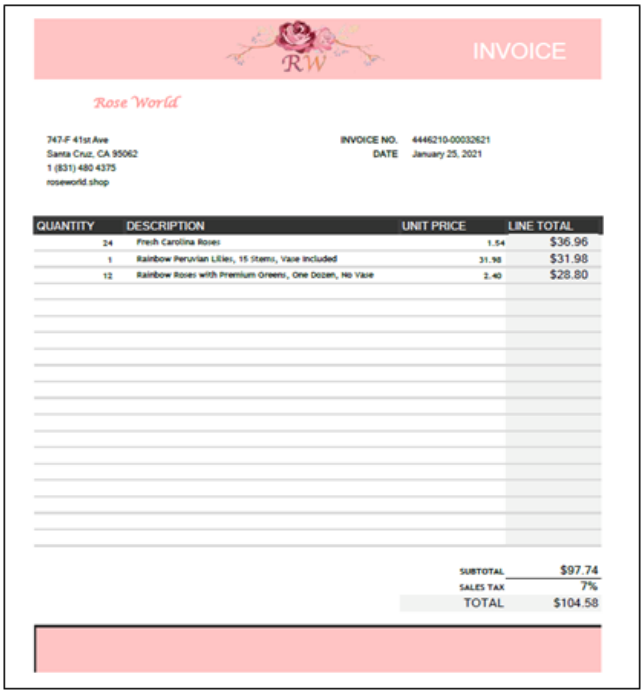


Figure 8: Invoice with website

Figure 9: Rose World contact page and enter your order number

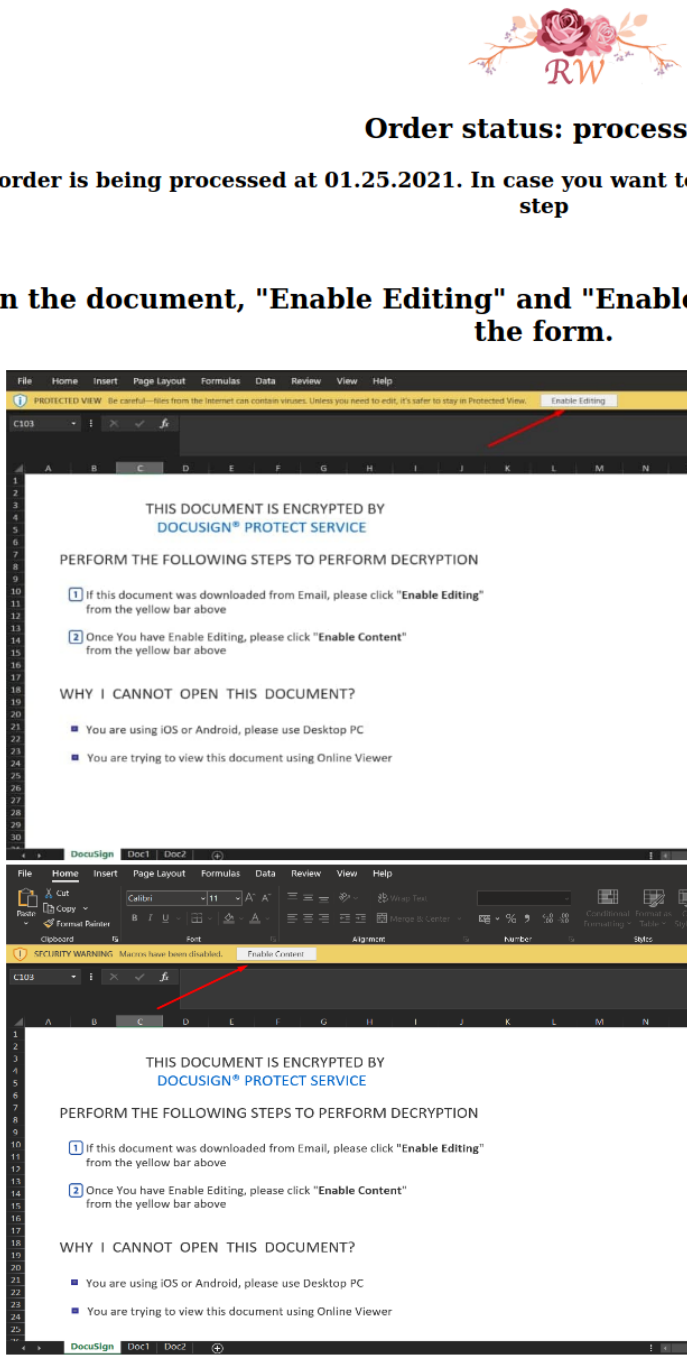


Figure 10: Enable Macros to receive Bazaloader

Conclusion:

Proofpoint researchers have observed a steady growth in actors using BazaLoader as a 1st stage downloader. In addition to the uptick in BazaLoader distribution, there is active development of BazaLoader, particularly during the month of October 2020. These recent BazaLoader campaigns exemplify affiliate actors leveraging a loader that is increasingly popular and more reliant on human interaction. Further, the social engineering features rely on the timeliness of the Valentine's Day holiday and the intrinsic user curiosity to see what they may have ordered. From a technical point of view, we have provided a number of IOCs and ET signatures below as this malware family is used to execute on any number of actor or affiliate intentions, actions, and objectives.

IOCs

IOC	IOC Type	Description	First Observed
hxxps[://]cacla2006[.]org/achlom/hamin[.]php	URL	Excel Payload	January 29, 2021
447b4c867b7147afe178d73adf8113fc33f6399f03707e4308efa36e0859bf86	SHA256	BazaLoader Hash	January 29, 2021
hxxps://52[.]12[.]160[.]92/exceed/requested7/ppd15	C&C	BazaLoader C&C	January 29, 2021
hxxps://34[.]220[.]204[.]73/exceed/requested7/ppd15	C&C	BazaLoader C&C	January 29, 2021
hxxps[://]www[.]cutedigitalphotography[.]com/vitrum/caretas[.]php	URL	Excel Payload	January 29, 2021
b6e5f8a1d01bfa0524707ed914409ccb6d28137f05467b3fccb52af02e510f34	SHA256	BazaLoader Hash	January 29, 2021
hxxps[://]18[.]188[.]232[.]155/leading/crisis26/snow11	C&C	BazaLoader C&C	January 29, 2021
hxxps[://]18[.]188[.]232[.]155/investigate/discharge/partially2	C&C	BazaLoader C&C	January 29, 2021
hxxps[://]homeprojectplanning[.]com/germes/sanertl[.]php	URL	Excel Payload	February 1, 2021
fd142ad1919c5ca254b75745739a72aaec509afdd74715139ecc60266d7fdd3e	SHA256	BazaLoader Hash	February 1, 2021
hxxps[://]52[.]12[.]160[.]92/blog/entry/361446	C&C	BazaLoader C&C	February 1, 2021
hxxps[://]52[.]12[.]160[.]92/goods/itemid/124324	C&C	BazaLoader C&C	February 1, 2021
hxxps[://]54[.]190[.]50[.]234/organization/round_table	C&C	BazaLoader C&C	February 1, 2021

hxxps[://]34[.]220[.]167[.]220/organization/round_table	C&C	BazaLoader C&C	February 1, 2021
hxxps[://]18[.]236[.]86[.]87/organization/round_table	C&C	BazaLoader C&C	February 1, 2021
hxxps[://]34[.]212[.]73[.]169/organization/round_table	C&C	BazaLoader C&C	February 1, 2021
hxxps[://]morrislibraryconsulting[.]com/favicam/gertnm[.]php	URL	Excel Payload	February 8, 2021
b4acd05efadb07351ad853233220bf7f5dd13fbc26fd065d56925c05a42f1927	SHA256	BazaLoader Hash	February 8, 2021
hxxps[://]34[.]210[.]71[.]206/news/article/12422	C&C	BazaLoader C&C	February 8, 2021
hxxps[://]34[.]210[.]71[.]206/artists/id/13131	C&C	BazaLoader C&C	February 8, 2021
hxxps[://]acegikbcggin[.]bazar/news/article/12422	C&C	BazaLoader C&C	February 8, 2021
hxxps[://]acegilbcggio[.]bazar/news/article/12422	C&C	BazaLoader C&C	February 8, 2021
hxxps[://]horsehospital[.]com/assebles/hamnab[.]php	URL	Excel Payload	February 8, 2021
b5d7dc4e53f5242e6354c9e20bba1e49d2b34261f706a8c9c9e1b6b18bff348b	SHA256	BazaLoader Hash	February 8, 2021
hxxps[://]34[.]210[.]71[.]206/home/static	C&C	BazaLoader C&C	February 8, 2021

ET Signatures

SID	Name
2844993	ETPRO TROJAN bazaloader Variant CnC Activity
2844992	ETPRO TROJAN bazaloader Variant CnC Activity
2844991	ETPRO TROJAN bazaloader Variant CnC Activity
2844795	ETPRO TROJAN bazaBackdoor Variant CnC (Checkin)
2844794	ETPRO TROJAN Possible bazaloader CnC Activity M3

2844766	ETPRO TROJAN Possible bazaloader CnC Activity M2
2844765	ETPRO TROJAN Possible bazaloader CnC Activity M1
2844764	ETPRO TROJAN SSL/TLS Certificate Observed (bazaloader)
2844763	ETPRO TROJAN SSL/TLS Certificate Observed (bazaloader)
2844355	ETPRO TROJAN Observed bazaLoader User-Agent
2844246	ETPRO TROJAN bazar Backdoor CnC Activity
2843035	ETPRO TROJAN bazaBackdoor Variant CnC Activity M3
2843034	ETPRO TROJAN bazaBackdoor Variant CnC Activity M2
2843033	ETPRO TROJAN bazaLoader Variant CnC Activity M1
2842090	ETPRO TROJAN bazaLoader CnC (Download Request)
2842073	ETPRO TROJAN bazaBackdoor Variant CnC (Checkin)
2031085	ET TROJAN bazaloader Variant Activity
2031084	ET TROJAN bazaloader Variant Activity
2030988	ET TROJAN Observed Malicious SSL Cert (bazaLoader CnC)
2030820	ET TROJAN Observed Malicious SSL Cert (bazar Backdoor)
2030270	ET TROJAN Observed Malicious DNS Query (bazarLoader/Team9 Backdoor CnC Domain)
2030269	ET TROJAN Observed Malicious DNS Query (bazarLoader/Team9 Backdoor CnC Domain)
2030268	ET TROJAN Observed Malicious DNS Query (bazarLoader/Team9 Backdoor CnC Domain)
2030267	ET TROJAN Observed Malicious DNS Query (bazarLoader/Team9 Backdoor CnC Domain)
2030045	ET TROJAN bazaR CnC Domain in DNS Lookup
2030044	ET TROJAN bazaR CnC Domain in DNS Lookup
2030043	ET TROJAN bazaR CnC Domain in DNS Lookup
2030042	ET TROJAN bazaR CnC Domain in DNS Lookup
2030041	ET TROJAN bazaR CnC Domain in DNS Lookup

2029973	ET INFO Observed DNS Query for EmerDNS TLD (.bazar)

Subscribe to the Proofpoint Blog