TA444: The APT Startup Aimed at Acquisition (of Your Funds)

proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds

January 23, 2023

Blog
Threat Insight
TA444: The APT Startup Aimed at Acquisition (of Your Funds)

January 25, 2023 Greg Lesnewich and the Proofpoint Threat Research Team

Key Takeaways

- TA444 is a North Korea state-sponsored threat actor that tested numerous infection methods in 2022 with varying degrees of success.
- TA444 is a unicorn among state-aligned actors as its primary operations are financially motivated, and their infection chains are often a microcosm of the cybercrime threat landscape at large.
- While TA444 has been active in its current form of targeting cryptocurrencies since at least 2017, the group has adopted an upstart mentality during the latter stages of 2022.

Overview

In the world of tech startups, luminaries and charlatans alike boast of the value of rapid iteration, testing products on the fly, and failing forward. TA444, a North Korea-sponsored advanced persistent threat group, has taken these mantras to heart. TA444, which overlaps with public activity called APT38, Bluenoroff, BlackAlicanto, Stardust Chollima, and COPERNICIUM, is likely tasked with generating revenue for the North Korean regime. That tasking has historically involved the targeting of banks to ultimately funnel cash to the Hermit Kingdom or handlers abroad. More recently, TA444 has turned its attention, much like the tech industry, to cryptocurrency. While we do not know if the group has ping pong tables or kegs of some overrated IPA in its workspace, TA444 does mirror the startup culture in its devotion to the dollar and to the grind.

Fail Fast with File Type Variations

Back in its infant interest with blockchain and cryptocurrency, TA444 had two main avenues of initial access: an LNK-oriented delivery chain and a chain beginning with documents using remote templates. These campaigns were typically referred to as DangerousPassword, CryptoCore, or SnatchCrypto. In 2022, TA444 continued to use both methods, but had also tried its hand at other file types for initial access. Despite having not heavily relied on macros in previous campaigns, TA444 seemed to mirror the cybercrime landscape in the summer and fall, attempting to find additional file types to stuff its payloads into.

It is unclear if the threat actor had a hackathon to generate these ideas, but we believe some of the (dramatized) conversations may have sounded like this:

MSI Installer files? Let's give it a shot but try a few varieties and see what sticks!

Virtual Hard Drive? TA580 used it to drop Bumblebee, why don't we have a VHD chain?

ISOs to bypass MoTW? If the market wants it, let's give it to them!

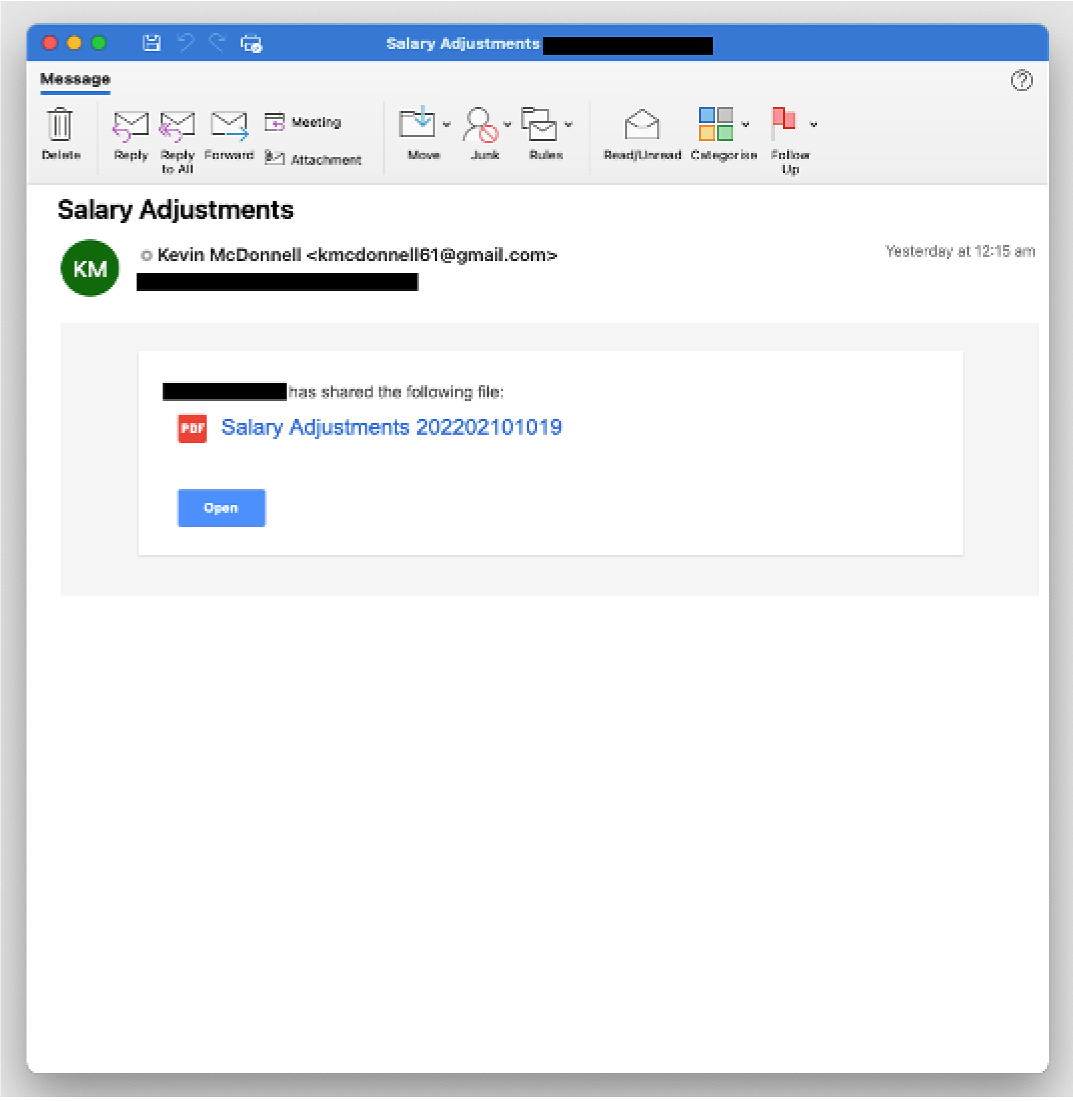
Compiled HTML? What are we, TA406? Eh, give it a try anyway!

We can experiment all we want but we must keep up with our CageyChameleon and Astraeus quotas to meet our OKRs!

Equally as surprising as the variance in delivery methods is the lack of a consistent payload at the end of the delivery chains. When other financially-oriented threat actors test delivery methods, they tend to load their traditional payloads; this is not the case with TA444. This suggests that there is an embedded, or at least a devoted, malware development element alongside TA444 operators.

What's Our Go-to-Market?

To convince victims to click on malicious links, TA444 has a complete marketing strategy to increase its chances of new ARR (Annual Recurring Revenue). It all starts with crafting lure content that may be of interest or necessity to the target. These can include analyses of cryptocurrency blockchains, job opportunities at prestigious firms, or salary adjustments.



Salary Adjustments [redacted]

Salary Adjustments

KM Kevin McDonnell <kmcdonnell61@gmail.com>

Yesterday at 12:15 am

[redacted]

[redacted] has shared the following file:

Salary Adjustments 202202101019

Figure 1. Example TA444 email lure using salary adjustment themes.

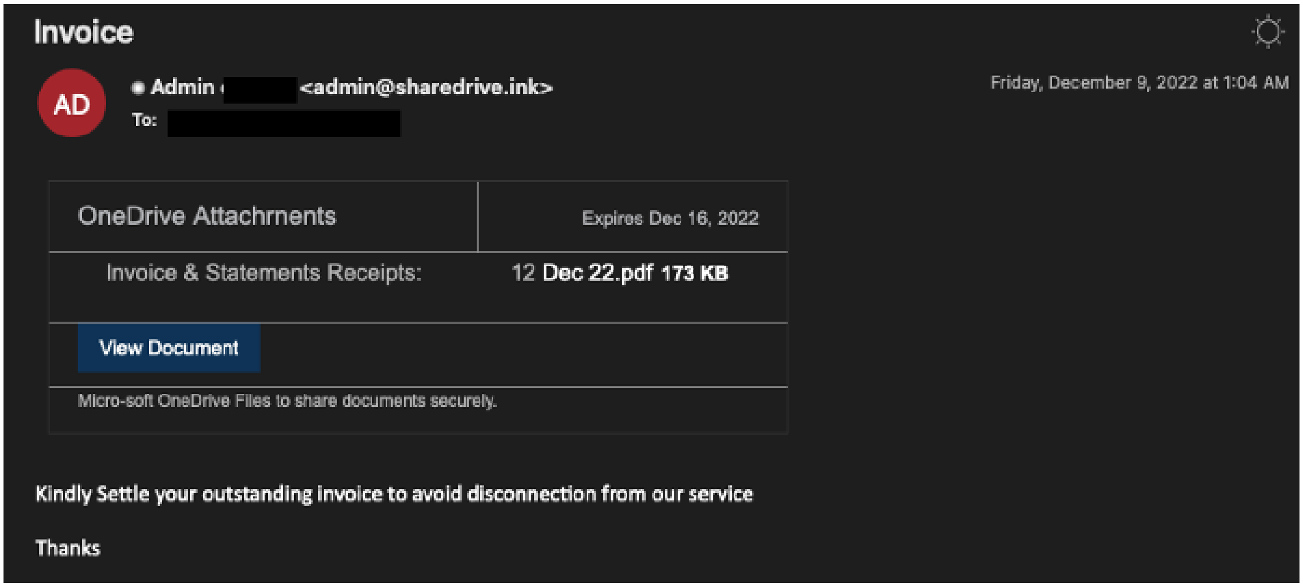
TA444 has abused email marketing tools like SendInBlue and SendGrid to engage with its target audience. These serve as redirectors to either cloud-hosted files or connect the victim directly to TA444 infrastructure. Additionally, the use of such links removes some stigma from the user of clicking on an unknown link, as marketing links will not necessarily get called out by phishing training.

Like other entities in the tech and cryptocurrency space, someone in TA444's organization oversees socials. This is a very strong component of TA444's practice, as the threat actor has continued to use LinkedIn to engage with victims prior to delivering links to malware. Proofpoint has observed this group demonstrating workable understandings of English, Spanish, Polish, and Japanese.

Test in Prod

In early December 2022, Proofpoint researchers observed a significant deviation from normal TA444 operations via a relatively basic credential harvesting campaign. A TA444 C2 domain sent OneDrive phishing emails rife with typos to a wide variety of targets in the United States and Canada, spanning several verticals including education, government, and healthcare, in addition to financial verticals. The lure emails enticed users to click a SendGrid URL which redirected to a credential harvesting page. The deviation in TA444's targeting and volume of messages made us thoroughly analyze the campaign to both understand the activity, but also challenged our assumptions about the group. This spam wave alone nearly doubled the total volume of TA444 email messages we had observed in our data during 2022, so we were concerned about false positive detection, as well as understanding a potential change in TA444 objectives.

The from header used the term Admin and the target domain name, but all used the same envelope-from email address (admin[@]sharedrive[.]ink) and subject (Invoice spelled with a lowercase L).



Invoice

Admin [redacted] <admin@sharedrive.ink>

To: [redacted]

Friday, December 9, 2022 at 1:04 AM

OneDrive Attachrnents — Expires Dec 16, 2022

Invoice & Statements Receipts: 12 Dec 22.pdf 173 KB

Micro-soft OneDrive Files to share documents securely.

Kindly Settle your outstanding invoice to avoid disconnection from our service

Thanks

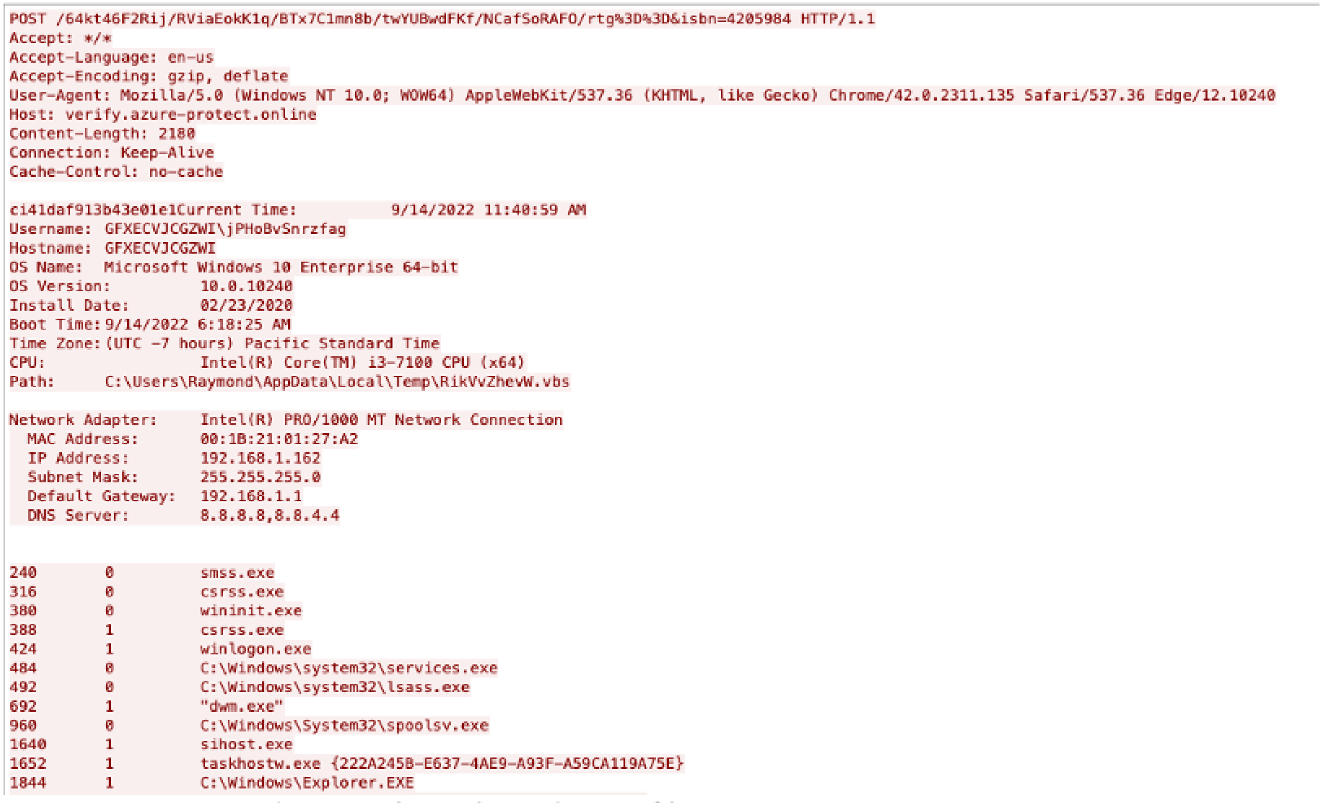
Figure 2. TA444 phishing email that deviated from expected themes and targeting.

The SendGrid URLs are used to redirect targets to the domain superiorexhbits[.]com which uses common phishing tactics such as loading the victim's iconography via the logo-rendering service ClearBit. This sprawling credential harvesting activity is a deviation from normal TA444 campaigns, which typically involve the direct deployment of malware. In fact, this same domain was observed serving a TA444 VHD containing Cur1Agent on the same day.

Proofpoint attributed this campaign with moderate to moderately high confidence based on the exclusivity of TA444 infrastructure. Other domains hosted on that IP match previous TA444 typo squats. The emails also had valid DMARC and SPF records, indicating that the sender has control of that domain. Proofpoint cannot rule out that the TA444 server was compromised by another actor to send the phishing links. It is also possible that TA444, like other North Korean actors such as Andariel, has begun its own moonlighting operations. If this occurred, we would anticipate seeing tool and infrastructure re-use as well as continued deviation of targeting away from major cryptocurrency and financial institutions.

The Culture is the Foundation

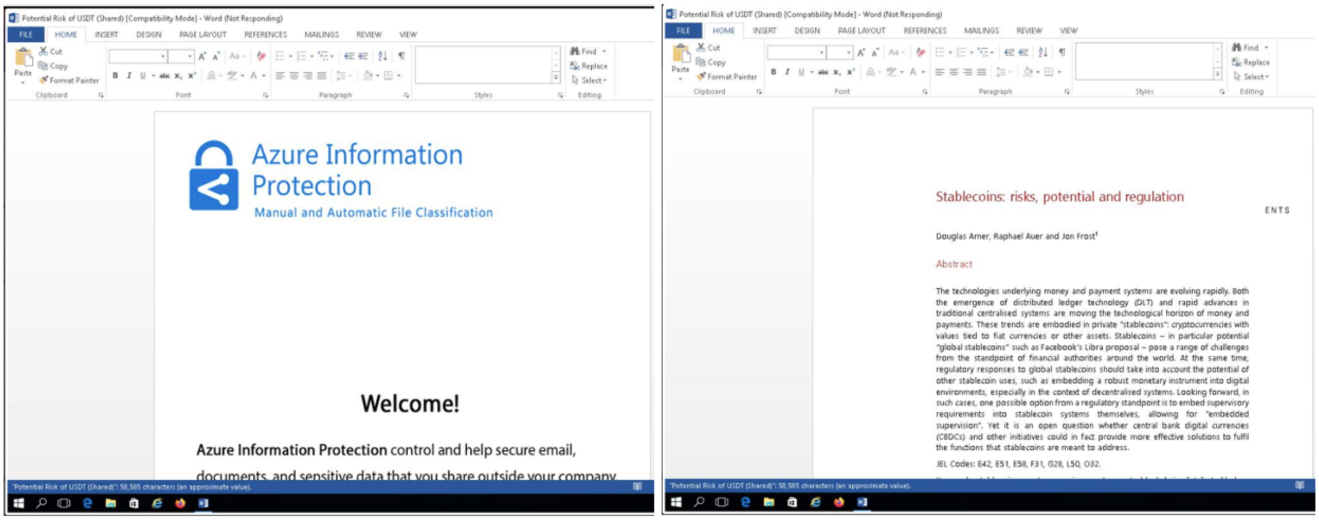
While TA444 has experimented with new lines of production, their core families still carry the brunt of their infections. The CageyChameleon (aka CabbageRAT) family has expanded its functionality but still operates as a victim-profiling framework, exfiltrating running processes and host information while setting up the potential to launch subsequent tooling loaded from the command-and-control server. The lure LNKs used to initiate execution are still often titled Password.txt.lnk.



```
POST /64kt46F2Rij/RViaEokK1q/BTx7C1mn8b/twYUBwdFKf/NCafSoRAFO/rtg%3D%3D&isbn=4205984 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.10240
Host: verify.azure-protect.online
Content-Length: 2180
Connection: Keep-Alive
Cache-Control: no-cache

ci41daf913b43e01e1Current Time:          9/14/2022 11:40:59 AM
Username:  GFXECVJCGZWI\jPHoBvSnrzfag
Hostname:  GFXECVJCGZWI
OS Name:   Microsoft Windows 10 Enterprise 64-bit
OS Version:          10.0.10240
Install Date:        02/23/2020
Boot Time:9/14/2022 6:18:25 AM
Time Zone:(UTC -7 hours) Pacific Standard Time
CPU:                 Intel(R) Core(TM) i3-7100 CPU (x64)
Path:      C:\Users\Raymond\AppData\Local\Temp\RikVvZhevW.vbs

Network Adapter:     Intel(R) PRO/1000 MT Network Connection
  MAC Address:       00:1B:21:01:27:A2
  IP Address:        192.168.1.162
  Subnet Mask:       255.255.255.0
  Default Gateway:   192.168.1.1
  DNS Server:        8.8.8.8,8.8.4.4


240        0         smss.exe
316        0         csrss.exe
380        0         wininit.exe
388        1         csrss.exe
424        1         winlogon.exe
484        0         C:\Windows\system32\services.exe
492        0         C:\Windows\system32\lsass.exe
692        1         "dwm.exe"
960        0         C:\Windows\System32\spoolsv.exe
1640       1         sihost.exe
1652       1         taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
1844       1         C:\Windows\Explorer.EXE
```

Figure 3. Decrypted CageyChameleon data exfiltration.

Similarly, TA444 has stayed the course with its infrastructure deployments and document content, effectively reusing lure iconography in second-stage macro-laden files and borrowing content directly from entities it is spoofing. First stage remote template files have adapted to not only download the second-stage macro (tracked as Astraeus by Proofpoint) but the first stage now contains an obfuscated Cardinal backdoor, as noted by PWC and Kaspersky.


Potential Risk of USDT (Shared) [Compatibility Mode] - Word (Not Responding)
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
Find
Replace
Select
Clipboard
Font
Paragraph
Styles
Editing
"Potential Risk of USDT (Shared)": 58,585 characters (an approximate value).

Azure Information Protection

Manual and Automatic File Classification

Welcome!

Azure Information Protection control and help secure email, documents, and sensitive data that you share outside your company

Stablecoins: risks, potential and regulation

ENTS

Douglas Arner, Raphael Auer and Jon Frost[1]

Abstract

The technologies underlying money and payment systems are evolving rapidly. Both the emergence of distributed ledger technology (DLT) and rapid advances in traditional centralised systems are moving the technological horizon of money and payments. These trends are embodied in private "stablecoins": cryptocurrencies with values tied to fiat currencies or other assets. Stablecoins – in particular potential "global stablecoins" such as Facebook's Libra proposal – pose a range of challenges from the standpoint of financial authorities around the world. At the same time, regulatory responses to global stablecoins should take into account the potential of other stablecoin uses, such as embedding a robust monetary instrument into digital environments, especially in the context of decentralised systems. Looking forward, in such cases, one possible option from a regulatory standpoint is to embed supervisory requirements into stablecoin systems themselves, allowing for "embedded supervision". Yet it is an open question whether central bank digital currencies (CBDCs) and other initiatives could in fact provide more effective solutions to fulfil the functions that stablecoins are meant to address.

JEL Codes: E42, E51, E58, F31, G28, L50, O32.

Figure 4. TA444 first-stage lure document themes.

Security researchers have observed TA444 deploying an impressive set of post-exploitation backdoors in its history, including msoRAT, Cardinal (default.rdp), the Rantankba suite, CHEESETRAY, and DYEPACK, as well as passive backdoors, virtualized listeners, and browser extensions to facilitate theft.

Attribution

Proofpoint clusters TA444 activities based on malware lineage, behavioral heuristics and traits of first-stage tooling meant to fool targeted users, distinctive infrastructure usage, and targeting of financial entities, along with other factors. Historic TA444 operations, such as the 2016 Bangladesh Bank heist and targeting of cryptocurrency entities, have been linked to the North Korean government by the United States.

The United States Treasury Department levied sanctions against two coin mixing services, Tornado Cash and BlenderIO, for allowing TA444 operators to launder over $120 million of cryptocurrency stolen from intrusions into various bridge and exchange entities. The US Federal Bureau of Investigation attributed the heist of a major cryptocurrency bridge to APT38, a group which heavily overlaps with TA444, where funds were later mixed in BlenderIO. This attribution underlines how reliant TA444 is on the cryptocurrency ecosystem to steal funds, create an avenue to launder them, and cash out. Recent TA444 activity highlights how willing the adversary is to adapt their methods to continue to profit from its intrusions, and new services will like aide them in their efforts, even if unintentionally.

Conclusion

While we may poke fun at its broad campaigns and ease of clustering, TA444 is an astute and capable adversary that is willing and able to defraud victims for hundreds of millions of dollars. TA444 and related clusters are assessed to have stolen nearly $400 million dollars' worth of cryptocurrency and related assets in 2021. In 2022, the group surpassed that value in a single heist worth over $500 million, gathering more than $1 billion during 2022. North Korea, like other cryptocurrency enthusiasts, has weathered the declining value of cryptocurrencies, but remains engaged in its efforts to use cryptocurrency as a vehicle to provide usable funds to the regime.

ET Signatures

2043279- ET MALWARE TA444 Related Domain in DNS Lookup (updatezone .org)

2043280- ET MALWARE TA444 Related Domain in DNS Lookup (autoprotect .com .de)

2043281- ET MALWARE TA444 Related Domain in DNS Lookup (autoprotect .gb .net)

2043282- ET MALWARE TA444 Related Domain in DNS Lookup (azure-security .online)

2043283- ET MALWARE TA444 Related Domain in DNS Lookup (azure-security .site)

2043284- ET MALWARE TA444 Related Domain in DNS Lookup (hoststudio .org)

2043285- ET MALWARE TA444 Related Domain in DNS Lookup (thecloudnet .org)

2037802- ET MALWARE TA444 Related Domain in DNS Lookup (documentworkspace .io)

2037803- ET MALWARE TA444 Related Domain in DNS Lookup (fclouddown .co)

2037804- ET MALWARE TA444 Related Domain in DNS Lookup (googlesheet .info)

2037883- ET MALWARE TA444 Related Domain in DNS Lookup (inst .shconstmarket .com)

2037884- ET MALWARE TA444 Related Domain in DNS Lookup (web .shconstmarket .com)

2037885- ET MALWARE TA444 Related Domain in DNS Lookup (wordonline .cloud)

2038542- ET MALWARE Observed DNS Query to TA444 Domain (cooporatestock .com)

2038543- ET MALWARE Observed DNS Query to TA444 Domain (finxiio .com)

2038544- ET MALWARE Observed DNS Query to TA444 Domain (1drvmicrosoft .com)

2038546- ET MALWARE Observed DNS Query to TA444 Domain (ledger-cloud .com)

2038547- ET MALWARE Observed DNS Query to TA444 Domain (globiscapital .co)

2038548- ET MALWARE Observed DNS Query to TA444 Domain (wpsonline .co)

2038709- ET MALWARE Observed DNS Query to TA444 Domain (wps .wpsonline .co)

2038710- ET MALWARE Observed DNS Query to TA444 Domain (documentshare .info)

2038711- ET MALWARE Observed DNS Query to TA444 Domain (unchained-capital .co)

2038712- ET MALWARE Observed DNS Query to TA444 Domain (cloud .globiscapital .co)

2038713- ET MALWARE Observed DNS Query to TA444 Domain (shconstmarket .com)

2038714- ET MALWARE Observed DNS Query to TA444 Domain (stablehouses .info)

2038715- ET MALWARE Observed DNS Query to TA444 Domain (edit .wpsonline .co)

2038716- ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .us .org)

2038717- ET MALWARE Observed DNS Query to TA444 Domain (salt1ending .com)

2038718- ET MALWARE Observed DNS Query to TA444 Domain (cloud .jbic .us)

2038720- ET MALWARE Observed DNS Query to TA444 Domain (share .anobaka .info)

2038721- ET MALWARE Observed DNS Query to TA444 Domain (vote .anobaka .info)

2038722- ET MALWARE Observed DNS Query to TA444 Domain (cloud .wpic .ink)

2038762- ET MALWARE Observed DNS Query to TA444 Domain (careersbankofamerica .us)

2038763- ET MALWARE Observed DNS Query to TA444 Domain (mufg .tokyo)

2038764- ET MALWARE Observed DNS Query to TA444 Domain (azure-protect .online)

2038785- ET MALWARE Observed DNS Query to TA444 Domain (azure-protection .cloud)

2038786- ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .nyc)

2038787- ET MALWARE Observed TA444 Domain (bankofamerica .nyc in TLS SNI)

2038788- ET MALWARE Observed TA444 Domain (azure-protection .cloud in TLS SNI)

2038789- ET MALWARE Observed TA444 Domain (careersbankofamerica .us in TLS SNI)

2038790- ET MALWARE Observed TA444 Domain (azure-protect .online in TLS SNI)

2038791- ET MALWARE Observed TA444 Domain (mufg .tokyo in TLS SNI)

2038845- ET MALWARE Observed DNS Query to TA444 Domain (cloud .tptf .ltd)

2038846- ET MALWARE Observed DNS Query to TA444 Domain (careers .bankofamerica .nyc)

2038847- ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .offerings .cloud)

2038848- ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .tel)

2038849- ET MALWARE Observed DNS Query to TA444 Domain (cloud .mufg .uk)

2038850- ET MALWARE Observed TA444 Domain (cloud .tptf .ltd in TLS SNI)

2038851- ET MALWARE Observed TA444 Domain (bankofamerica .tel in TLS SNI)

2038852- ET MALWARE Observed TA444 Domain (cloud .mufg .uk in TLS SNI)

2038853- ET MALWARE Observed TA444 Domain (bankofamerica .offerings .cloud in TLS SNI)

2038854- ET MALWARE Observed TA444 Domain (careers .bankofamerica .nyc in TLS SNI)

2038919- ET MALWARE Observed DNS Query to TA444 Domain (docuprivacy .com)

2038920- ET MALWARE Observed DNS Query to TA444 Domain (share .anobaka .info)

2038921- ET MALWARE Observed DNS Query to TA444 Domain (privacysign .org)

2038922- ET MALWARE Observed DNS Query to TA444 Domain (ms .onlineshares .cloud)

2038923- ET MALWARE Observed DNS Query to TA444 Domain (team .msteam .biz)

2038924- ET MALWARE Observed DNS Query to TA444 Domain (mizuhogroup .us)

2038925- ET MALWARE Observed DNS Query to TA444 Domain (docs .azurehosting .co)

2038926- ET MALWARE Observed DNS Query to TA444 Domain (tptf .fund)

2038927- ET MALWARE Observed DNS Query to TA444 Domain (perseus .bond)

2038928- ET MALWARE Observed DNS Query to TA444 Domain (smbcgroup .us)

2038929- ET MALWARE Observed DNS Query to TA444 Domain (tptf .cloud)

2038936- ET MALWARE Observed TA444 Domain (tptf .fund in TLS SNI)

2038937- ET MALWARE Observed TA444 Domain (docs .azurehosting .co in TLS SNI)

2038938- ET MALWARE Observed TA444 Domain (team .msteam .biz in TLS SNI)

2038939- ET MALWARE Observed TA444 Domain (share .anobaka .info in TLS SNI)

2038940- ET MALWARE Observed TA444 Domain (smbcgroup .us in TLS SNI)

2038941- ET MALWARE Observed TA444 Domain (perseus .bond in TLS SNI)

2038942- ET MALWARE Observed TA444 Domain (docuprivacy .com in TLS SNI)

2038943- ET MALWARE Observed TA444 Domain (privacysign .org in TLS SNI)

2038944- ET MALWARE Observed TA444 Domain (mizuhogroup .us in TLS SNI)

2038945- ET MALWARE Observed TA444 Domain (ms .onlineshares .cloud in TLS SNI)

2038946- ET MALWARE Observed TA444 Domain (tptf .cloud in TLS SNI)

2038987- ET MALWARE TA444 Related Domain in DNS Lookup (onlinecloud .cloud)

2039041- ET MALWARE TA444 Domain in DNS Lookup (mufg .ink)

2039042- ET MALWARE TA444 Domain in DNS Lookup (mufg .us .org)

2039043- ET MALWARE Observed TA444 Domain (mufg .ink in TLS SNI)

2039044- ET MALWARE Observed TA444 Domain (mufg .us .org in TLS SNI)

2039808- ET MALWARE TA444 Domain in DNS Lookup (gdocshare .one)

2039809- ET MALWARE Observed TA444 Domain (gdocshare .one in TLS SNI)

2039823- ET MALWARE TA444 Domain in DNS Lookup (sharedrive .ink)

2039824- ET MALWARE TA444 Domain in DNS Lookup (dnx .capital)

2039825- ET MALWARE Observed TA444 Domain (sharedrive .ink in TLS SNI)

2039826- ET MALWARE Observed TA444 Domain (dnx .capital in TLS SNI)

Previous Blog Post
Subscribe to the Proofpoint Blog