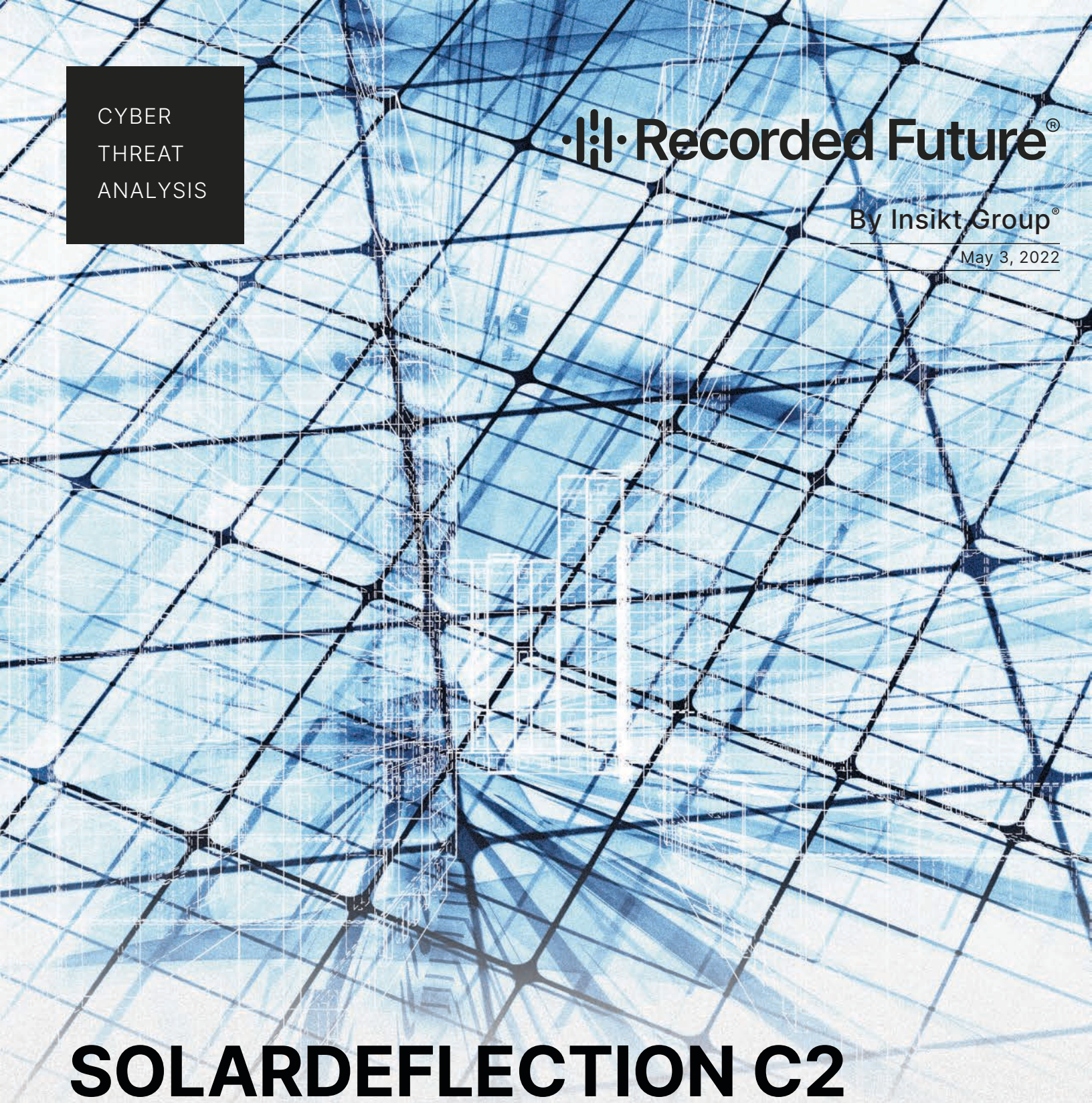


CYBER
THREAT
ANALYSIS

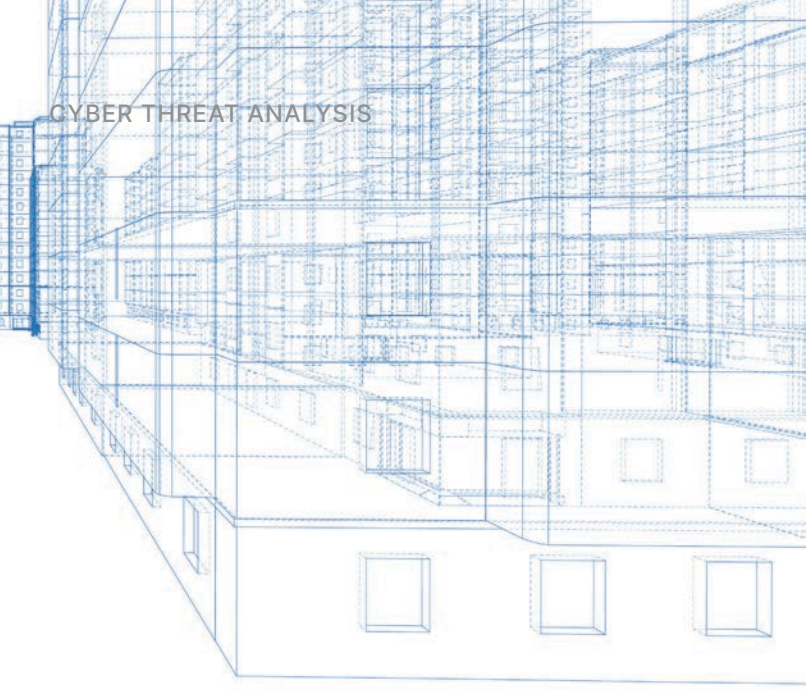
Recorded Future®

By Insikt Group®

May 3, 2022

SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse

Recorded Future®



This report profiles the unique infrastructure used by Russian state-sponsored threat activity group NOBELIUM. The activity was identified through a combination of large-scale automated network traffic analytics and analysis derived from open source reporting. Data sources include the Recorded Future Platform, SecurityTrails, DomainTools, PolySwarm, Farsight, Shodan, Censys, Team Cymru's Pure Signal™ and other common open-source tools and techniques. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to the activities of the Russian government in cyberspace and network defenders. Some technical details from our original research have not been included in this report version in order to protect tracking techniques and ongoing research into NOBELIUM activity.

Executive Summary

Recorded Future's Insikt Group continues to monitor Russian state-sponsored cyber espionage operations targeting government and private sector organizations across multiple geographic regions. From mid-2021 onwards, Recorded Future's midpoint collection revealed a steady rise in the use of NOBELIUM infrastructure tracked by Insikt Group as SOLARDEFLECTION, which encompasses command and control (C2) infrastructure. In this report, we highlight trends observed by Insikt Group while monitoring SOLARDEFLECTION infrastructure and the recurring use of typosquat domains by its operators.

A key factor we have observed from NOBELIUM operators involved in threat activity is a reliance on domains that emulate other brands (some legitimate and some that are likely fictitious businesses). Domain registrations and typosquats can enable spearphishing campaigns or redirects that pose a threat to victim networks and brands.

Using a combination of proactive adversary infrastructure detections, domain analysis techniques, and Recorded Future Network Traffic Analysis, we have determined that NOBELIUM's use of SOLARDEFLECTION infrastructure overlaps with other common infrastructure tactics, techniques, and procedures (TTPs) previously attributed to the group by multiple organizations including Microsoft, Fortinet, Sekoia, and Volexity. Previous open source reporting also highlighted NOBELIUM's use of cracked versions of the Cobalt Strike penetration testing tool.

Key Judgments

- Insikt Group is confident that the identified SOLARDEFLECTION infrastructure can be attributed to the threat activity group publicly reported as NOBELIUM; this confidence is based on the use of overlapping network infrastructure previously attributed to NOBELIUM in public reporting, as well as unique variations of Cobalt Strike traditionally used by the group.
- Broader themes in SOLARDEFLECTION C2 typosquats have included the misuse of brands across multiple industry verticals, particularly in the news and media industries.
- Cobalt Strike servers related to SOLARDEFLECTION monitoring that were also previously linked to NOBELIUM activity used modified server configurations, likely in an attempt to remain undetected from researchers actively scanning for standard Cobalt Strike server features.
- NOBELIUM has made extensive use of typosquat domains in SSL certificates and will likely continue to use deceptive techniques, including typosquat redirection, when using Cobalt Strike tooling.

Background

Analysis of recent and historical domains attributed to NOBELIUM broadly demonstrates the group's familiarity with, and tendency to emulate, a variety of media, news and technology providers. The group has abused dynamic DNS resolution to construct and resolve to randomly generated subdomains for its C2s or root domains to mislead victims. The key aspect to these attacks is the use of either email addresses or URLs that look similar to the domain of a legitimate organization. Potentially harmful domain registrations and typosquats can enable spearphishing campaigns or redirects that pose an elevated risk to a company's brand or employees. A successful spearphish is dependent on factors such as the quality of the message, the credibility of the sender address, and, in the case of a redirecting URL, the credibility of the domain name. Insikt Group has previously observed other Russian nexus groups using typosquatting in support of operations, such as those aimed at the 2020 presidential elections, to increase confidence in the validity of the fraudulent login portal used to harvest victim credentials. This tactic has also been reported recently in open sources in connection with intrusions targeting entities in Ukraine, likely in support of Russia's invasion of the country.

Figure 1: SOLARDEFLECTION Domain Registration reference in the Recorded Future Platform (Source: Recorded Future)

Insikt Group assesses that NOBELIUM is a threat activity group operating in line with the objectives of Russia's Foreign Intelligence Service (SVR). The SVR is tasked with providing the president of the Russian Federation, the Federal Assembly, and the government with the intelligence they need to make decisions in the areas of politics, the economy, military strategy, scientific-technical strategy, and the environment. Russia's SVR defines itself as separate by allowing the Russian Main Intelligence Directorate (GRU) to focus on military intelligence operations, while the SVR focuses on political intelligence; this is, however, a very high-level view of these operations. The SVR conducts its affairs by collecting information via public and private means, with the intended goal of gathering strategic information from organizations and individuals who in turn influence strategic policy and decision-makers in targeted countries.

In 2021, Volexity published research outlining a suspected APT29 phishing operation that targeted non-governmental organizations (NGOs), research institutions, governments, and international bodies using election fraud-themed lures purporting to be sent from the United States Agency for International Development (USAID), a government agency. The same day, Microsoft also published research on wider TTPs used in the same campaign and attributed the activity to NOBELIUM, the group behind the SolarWinds intrusions. This campaign targeted sensitive diplomatic and government entities as early as February 2021. They believe the threat actor used this information to launch other highly targeted attacks as part of their broader campaign. Additional research confirmed that a cluster of infrastructure monitored by Insikt Group under the designation SOLARDEFLECTION since 2021 overlaps with this previous reporting. Ongoing detections within the Recorded Future Command and Control security feed assisted in confirming the registration of new typosquat domains tied to NOBELIUM operations. More notably, we have confirmed that several newly identified typosquats continue to adopt the naming conventions or themes that were originally flagged as likely being associated with NOBELIUM reporting as early as 2020.

The Recorded Future Platform automatically detects typosquatted domains; each newly created domain entity is evaluated for typosquatting-style similarity to other domains observed by Recorded Future. An example of this is the SOLARDEFLECTION typosquat displayed in Figure 1, which based on the domain's spelling was very likely an attempt by NOBELIUM operators to emulate the T-Mobile brand. A review of the frequency in which SOLARDEFLECTION domains were registered over the past two years confirmed NOBELIUM's tendency to register domains in cycles, occasionally taking short hiatuses which at times likely coincided with new open source reporting attributing several domains to NOBELIUM activity (as depicted within the Recorded Future timeline below).

Insikt Group proactively detects SOLARDEFLECTION infrastructure through an in-depth understanding of the infrastructure TTPs that the group employs (detailed further below within the Infrastructure TTPs section). Additionally, the Command and Control data set enables us to enrich and identify any SOLARDEFLECTION IPs that we have categorized as "positive C2". We then analyze network communications to investigate how the C2 is interacting with infected machines or how it is being administered by the adversary. SOLARDEFLECTION C2s can be reviewed from within the Recorded Future Platform's Command and Control data set.

Threat Analysis

SOLARDEFLECTION Overview

NOBELIUM employs a wide range of bespoke tooling developed in a variety of programming languages, demonstrating a substantial research and development effort in support of its cyber operations. The threat group also makes good use of publicly available commodity tools such as Cobalt Strike to hinder attribution efforts. NOBELIUM exhibits highly developed operational security practices in its tradecraft, aimed at disrupting researchers' efforts in associating their malware and infrastructure to the group. Using a combination of proactive C2 detections, domain analysis, and network traffic analysis, we have determined that SOLARDEFLECTION servers share common infrastructure TTPs, enabling us to confidently cluster and attribute these servers to NOBELIUM.

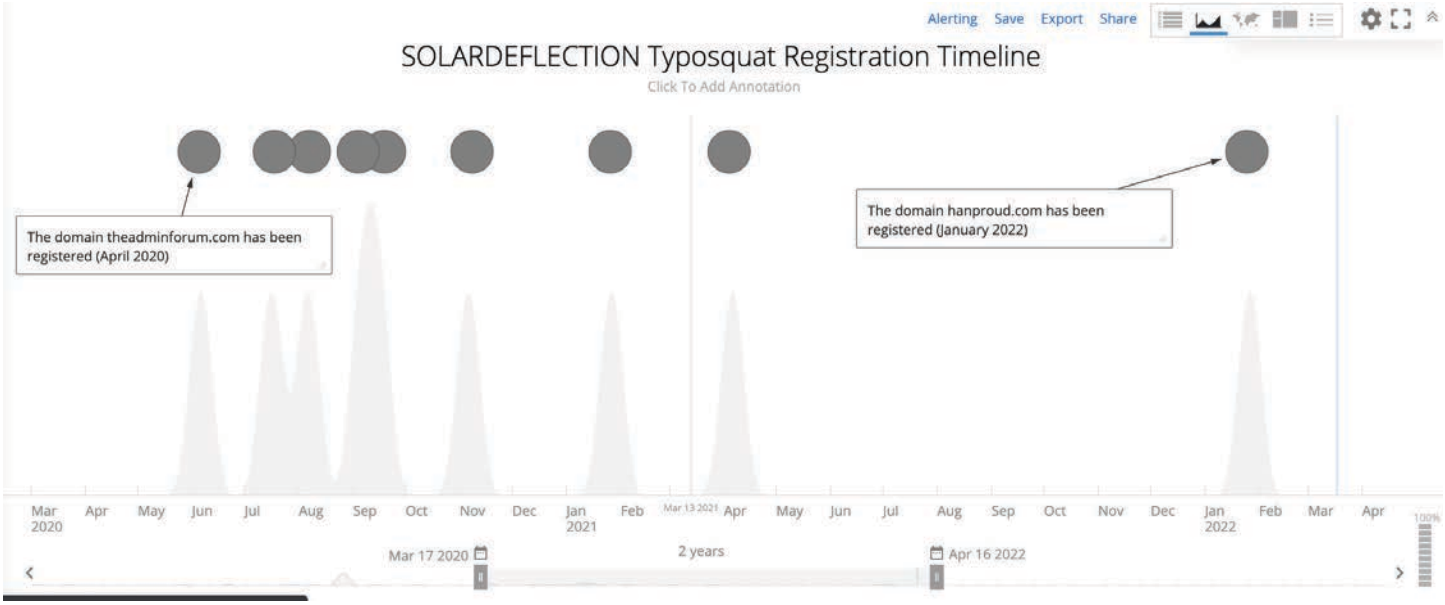


Figure 2: SOLARDEFLECTION Typosquat Registration Timeline (Source: Recorded Future Data)

Using current DNS records and passive DNS sources, we resolved IPs for newly registered domains tracked as SOLARDEFLECTION since January 2022 and reviewed SSL certificate information associated with these IPs. As a result, we discovered several domains via SOLARDEFLECTION tracking (see Appendix A) and a continued trend of using both Namesilo and Namecheap for domain registration. The reason behind the preference for these registrars is unknown; all domains collected under SOLARDEFLECTION had domain privacy options enabled.

Analysis of the domains covered under SOLARDEFLECTION highlighted a trend around the use of themed domains, primarily emulating entities within the media and news industry, as well as a smaller nexus around business development-themed domains. Both of these themes have been documented in open source reporting in connection with known NOBELIUM activity. The reason behind these theme choices is not fully understood beyond the suspected attempt to masquerade as other brands to appear legitimate to targets.

LUNARREFLECTION

While developing our original detection logic for SOLARDEFLECTION, we observed a secondary cluster of infrastructure that deviated technically from the main cluster. However, it contained domains bearing similarities to those used within SOLARDEFLECTION, and we believe this cluster is also likely managed by NOBELIUM operators. The similarities include the use of registrars Namecheap and Namesilo and domain themes that overlap with those identified within SOLARDEFLECTION domain registrations. Recorded Future tracks this secondary cluster under the name LUNARREFLECTION. An aggregation of discovered LUNARREFLECTION C2s is provided in Appendix A.

As seen in the industry breakdown in Figure 4 below, there is a similar trend among LUNARREFLECTION domains that emulate entities within the news and media industries. However, given the volume of SOLARDEFLECTION and LUNARREFLECTION typosquats in these industries, it is important to emphasize that the industry being emulated does not necessarily equate to that industry being targeted. Domains themed around news and media industry contacts are very likely to be used to target entities across a wider spectrum of industries, including those that have been consistently of interest to NOBELIUM operators, such as government embassies.

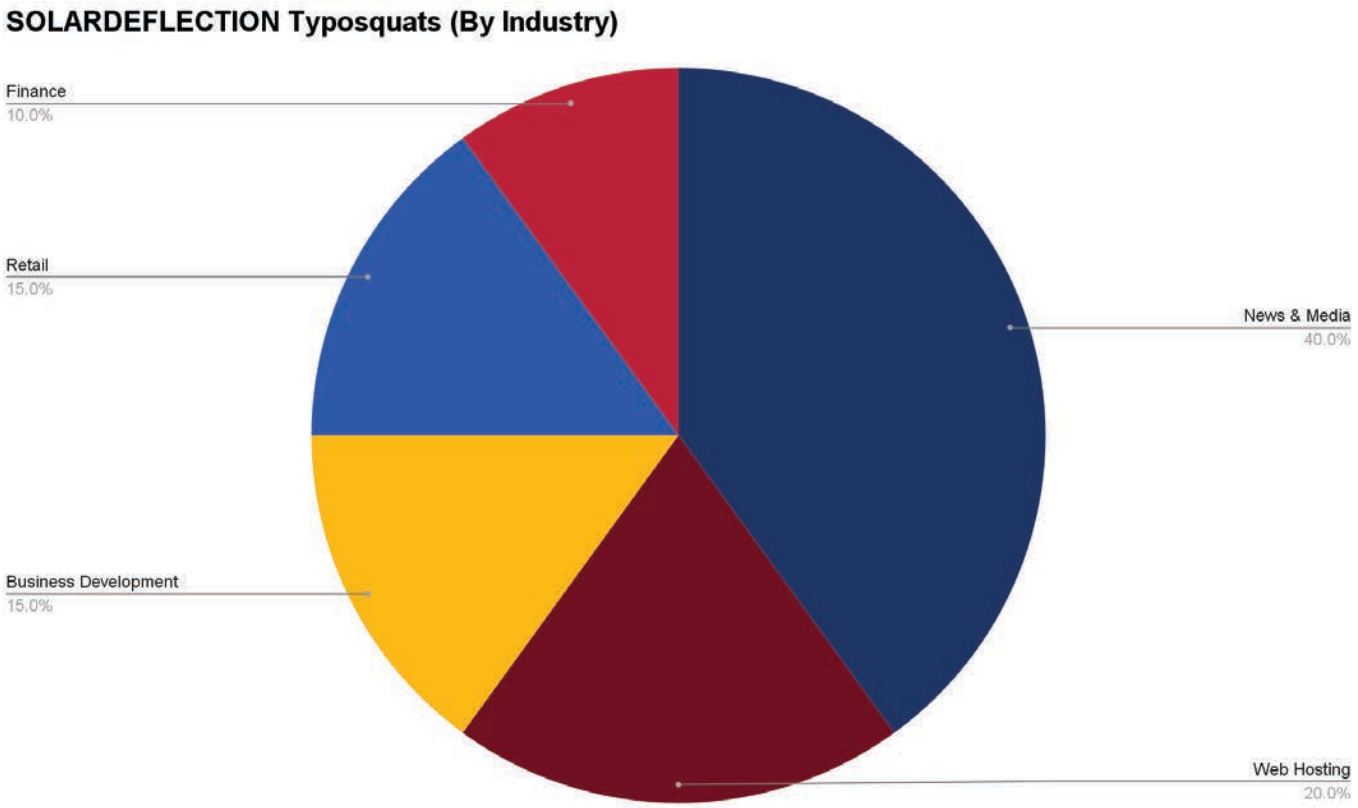


Figure 3: Breakdown of industries being emulated within SOLARDEFLECTION typosquats (Source: Recorded Future)

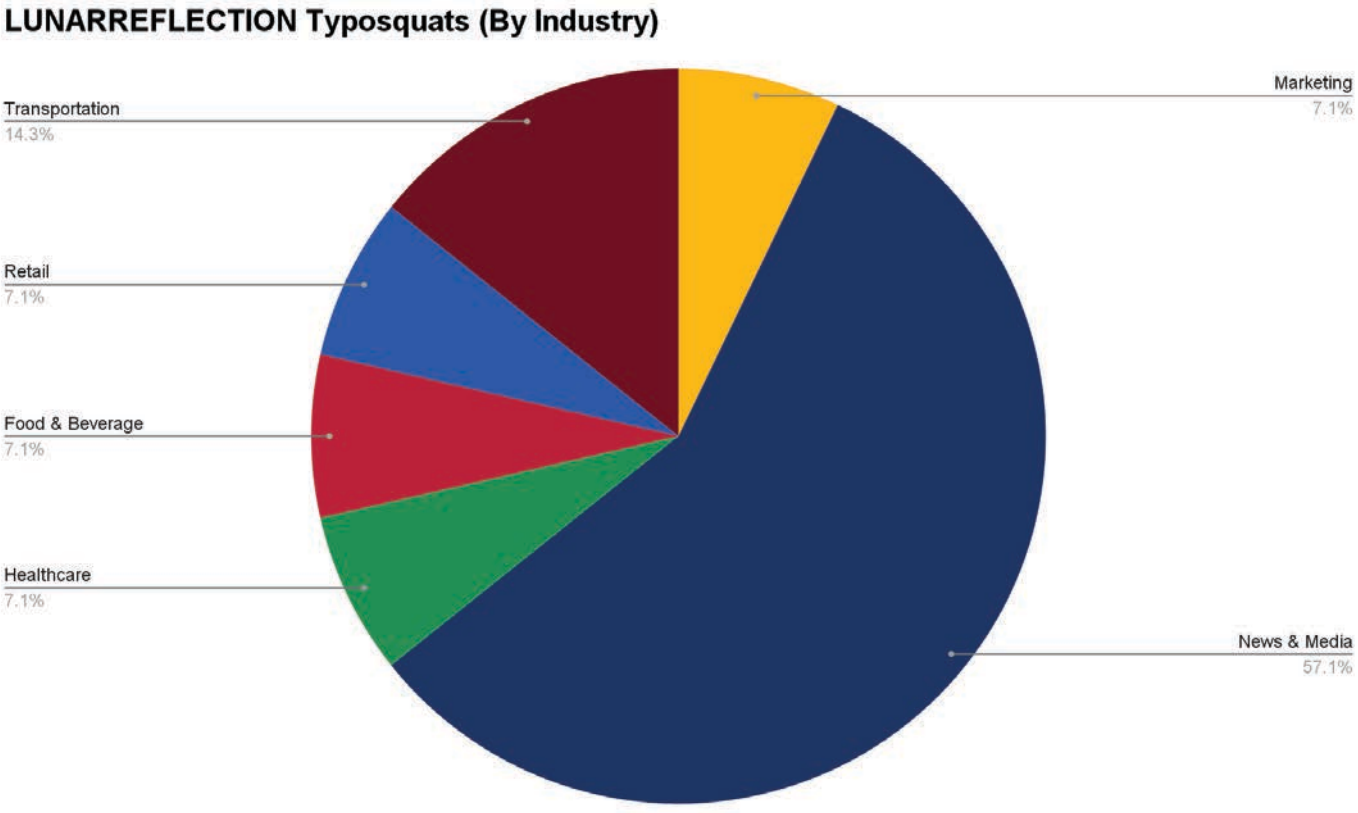


Figure 4: Breakdown of industries being emulated within LUNARREFLECTION typosquats (Source: Recorded Future)

Infrastructure TTPs

Recorded Future continues to monitor NOBELIUM by distilling vast swaths of open source and technical data and combining it with analysts' intimate knowledge of attacker tradecraft. Network Traffic Analysis analytics enable users to investigate and track suspected targeted intrusion activity derived from validated technical data sources. We apply a series of filters and algorithms to spot suspicious network traffic concerning these detected malicious servers, highlighting possible targeted intrusion activity. Intelligence Card extensions within the Recorded Future Platform then allow users to enrich this information further using data from close partners such as SecurityTrails, thereby enabling Recorded Future Threat Intelligence module users to efficiently map out prospective adversary campaigns.

Over the course of our research, Insikt Group observed multiple uncommon characteristics unique to NOBELIUM that serve as distinguishable hallmarks in terms of our potential to track this activity long term. The elements described below are some of the trackable characteristics which have been found to be used when investigating NOBELIUM-linked infrastructure with the resulting derived infrastructure covered under SOLARDEFLECTION and LUNARREFLECTION.

When analyzing SOLARDEFLECTION- and LUNARREFLECTION-related HTTP banner data, significant mistakes were observed and were found to be consistent across all related discovered infrastructure. A related trend involves the consistent use of specifically customized SSL certificates. Although these customizations are not unique to only SOLARDEFLECTION and LUNARREFLECTION instances on their own, the particular curation style of these certificates is uncommon and is a practice found consistently across all discovered infrastructure.

Also found consistently in SOLARDEFLECTION and LUNARREFLECTION infrastructure is a mismatch between the SSL certificate Subject CN (Common Name) and the 302 redirection location. Further investigation of the redirect location domain shows that the referenced URI is a legitimate resource for a fully functioning website; however, the Subject CN-related domain is typically found to have no significant website data associated with it.

Activity Spotlight: Role of Cobalt Strike

Some of the key characteristics used for SOLARDEFLECTION and LUNARREFLECTION have been the prevalent use of specific Cobalt Strike instances, including custom payload configurations, unique SSL certificates, and the likely use of cs2modrewrite to obfuscate C2 traffic. Cobalt Strike servers previously linked to NOBELIUM activity used modified server configurations to remain undetected by security researchers monitoring for standard Cobalt Strike server features. NOBELIUM has made extensive use of typosquat domains in SSL certificates and has used deceptive techniques including redirection when using Cobalt Strike tooling.

Analyzing infrastructure clustered under SOLARDEFLECTION and LUNARREFLECTION revealed hallmarks that pointed to the likely use of cs2modrewrite, a modification technique for Cobalt Strike-based infrastructure developed by members of Threat Express, an information security blog "created by red teamers, penetration testers and security professionals".

Details of the functionality of cs2modrewrite from its GitHub repository state, "This project converts a Cobalt Strike profile to a functional mod_rewrite .htaccess or Nginx config file to support HTTP reverse proxy redirection to a Cobalt Strike TeamServer. The use of reverse proxies provides protection to backend C2 servers from profiling, investigation, and general internet background radiation". Infrastructure linked to cs2modrewrite instances can be set up in several different ways, including separating the hosting of the reverse proxy server and Cobalt Strike server, or co-hosting the reverse proxy and Cobalt Strike on the same server.

Of particular interest in the repository is the file "cs2nginx.py", which was last updated February 5, 2020, and whose comment description states, "Converts Cobalt Strike profiles to Nginx config file format (/etc/nginx/nginx.conf)". The resulting Nginx configs will "Attempt to serve files locally if they exist", "Proxy any matching URIs to the C2 server", and "Redirect any non-matching requests to a specified redirection domain along with the original URI".

Analysis of cs2nginx functionality and comments reveals options for modification to Nginx Cobalt Strike servers that match infrastructure discovered via SOLARDEFLECTION. Insikt Group identified several methods of identifying network infrastructure used by NOBELIUM in their intrusion operations, based on the information published by Microsoft and analysis of the groups' infrastructure TTPs such as banner data.

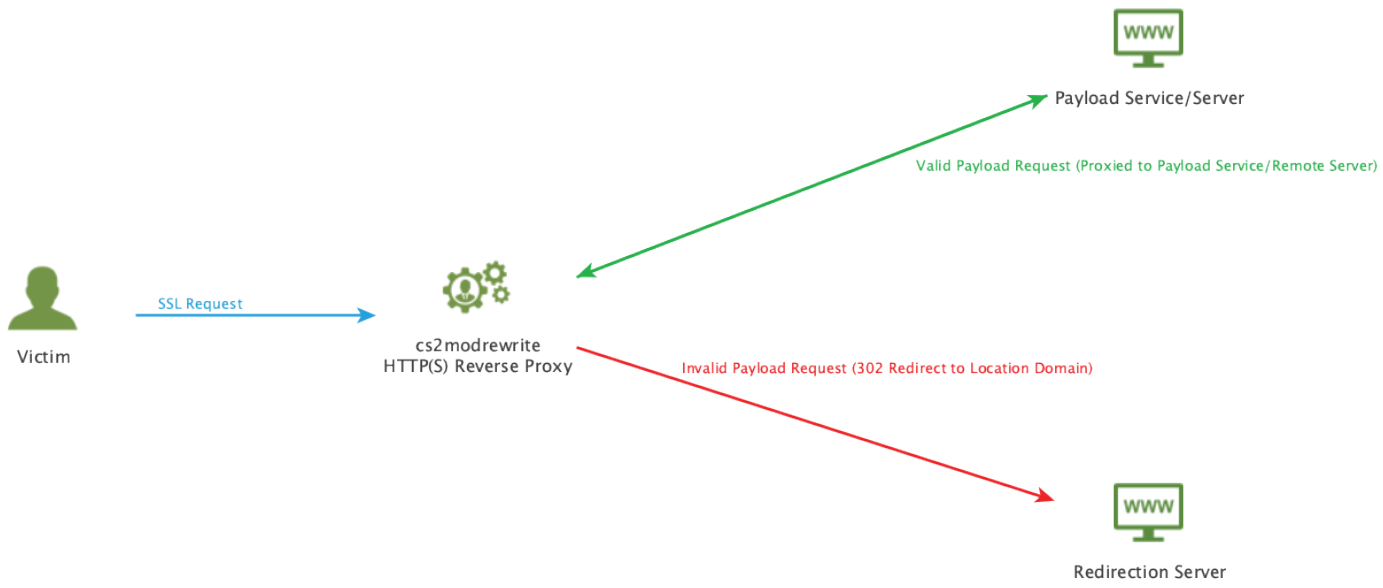


Figure 5: *cs2modrewrite Redirection method (Source: Maltego)*

Recurring Use of COSMICNODE

Analysis of NOBELIUM infrastructure identified multiple loader samples written using unique unpacking code used to deploy Cobalt Strike Beacons and shellcode that Insikt Group internally tracks as COSMICNODE. COSMICNODE is likely an evolution of the family tracked by Sentinel One in connection with NobleBaron and by Microsoft as NativeZone. Microsoft has previously stated that NativeZone encompasses multiple instances of NOBELIUM's custom Cobalt Strike loaders, making it an umbrella term for any variant, to include one of the several named families detailed further below. COSMICNODE typically uses rundll32.exe to load and execute follow-on payload(s).

As of this publication, the COSMICNODE family continues to use new anti-analysis, encryption, and obfuscation methods to disguise the Cobalt Strike payloads and hamper static detection of the COSMICNODE implants. NOBELIUM has used AES encryption, byte swapping, multi-stage XOR encoding, and other obfuscation methods, suggesting a deep understanding of how to hinder defender efforts to detect and analyze payloads. Malleable Cobalt Strike C2 Profiles enable operators to customize the details of the command and control protocol used. The Cobalt Strike payloads have predominantly used one of two watermarks associated with leaked builds, 1359593325 or 305419896, and the standard jQuery malleable profile that helps traffic blend in by mimicking legitimate services. The previously mentioned theme around typosquats of news-related entities carried over into both SOLARDEFLECTION and LUNARREFLECTION C2 server URLs that contained similar strings pertaining to "news" or "info" topics, including:

- sampledomain[.]com**,/news/update/aaa**
- sampledomain[.]com,**/news_indexedimages_autrzd/**

Infrastructure that did not meet the criteria for either SOLARDEFLECTION or LUNARREFLECTION, but matched signaturing for cs2modrewrite instances, which are likely to be Cobalt Strike servers, are aggregated in Appendix A.

Victimology

With the finite data available to Recorded Future surrounding this campaign, limited conclusions can be drawn regarding victimology. Through behavioral profiling of network traffic to adversary infrastructure, we were able to determine a clear and consistent pattern of SOLARDEFLECTION operators relying on Tor to obfuscate network traffic.

Overlaps with the HTML variant of EnvyScout detailed by Sekoia[.]io and findings from other researchers provide invaluable insight into likely lures such as those suspected to have targeted multiple embassies. Following this first discovery, other similar HTML files reported by Sekoia confirmed a possible targeting theme centered on "Covid information" based on the title of an HTML file they attributed to this campaign. This aligns with the themes of the phishing emails they attributed to this campaign, likely targeting embassies that pretended to be providing a status update about embassy operations in response to the pandemic.

Mitigations

The delivery of the Cobalt Strike Beacon malware and the C2 communication (defined by the malleable C2 profile) are best detected using intrusion detection systems (IDS) like Snort. We recommend that users conduct the following measures to detect and mitigate activity associated with SOLARDEFLECTION:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Recorded Future proactively detects and logs malicious server configurations in the Command and Control Security Control Feed. The Command and Control list includes tools used by NOBELIUM and other Russian state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence module users can monitor real-time output from Network Traffic Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence (BI) module. The SecurityTrails extension is available to any customer that has a subscription to the Threat Intelligence or Brand Intelligence modules. The LogoType source and alerting is exclusive to the BI module, though the TI module does have access to the data via the Advanced Query Builder.

Outlook

As tensions continue to rise in Eastern Europe, we expect to see a continuation of cyber operations being conducted by Russian-nexus groups, likely including NOBELIUM, in line with national strategic interests. Russia will likely also continue to exert influence over other governments, which may lead to additional computer network operations aimed at furthering strategic advantage. Typosquatting is likely to remain an integral technique for multiple threat entities supporting Russian national interests in the near future. Insikt Group has already observed groups that support these interests weaponize domains themed around Russia's invasion of Ukraine to great effect. This likely includes not only the domains belonging to one organization, but third-party partners and vendors with enterprise network access.

Appendix A — Indicators

The following tables contain domains deemed or assessed as malicious under the heading "X.509 Certificate Domain (Typosquat)", and their non-malicious associated redirect domains, under the heading "Location Domain". All domains detailed in these tables should not be used to infer targeting of their respective affiliation. As detailed within the body of this reporting, several of the domains identified in this appendix have previously been reported by other security researchers since mid-2021, which have assisted in corroborating Insikt Group's findings.

SOLARDEFLECTION Domains		
Location Domain	**X.509 Certificate Domain (Typosquat)**	**Registrar**
https://www[.]businessandit[.]com	60daybusinessaudit[.]com	NAMESILO, LLC
https://www[.]vmware[.]com	alifemap[.]com	NAMECHEAP INC
https://www[.]news[.]com	an-4news[.]com	NAMECHEAP INC
https://www[.]newsreview[.]com	cbdnewsandreviews[.]net	NAMESILO, LLC
https://celebs-infor[.]blogspot[.]com	celebsinformation[.]com	NAMESILO, LLC
https://www[.]ohiocpa[.]com	cityloss[.]com	NAMECHEAP INC
https://www[.]crochet[.]com	crochetnews[.]com	NAMESILO, LLC
https://e-blogpro[.]blogspot[.]com	eblogpro[.]com	NAMESILO, LLC
https://fashionweekdaily[.]com/category/news	fashionnewsarticles[.]com	NAMECHEAP INC
https://www[.]startabusinessfast[.]com	faststartbusiness[.]com	NAMESILO, LLC
https://www[.]gallatinnews[.]com	galatinonews[.]com	NAMECHEAP INC
https://www[.]facebook[.]com/Global-Trade-Motors-1603628046591244	globaltrademotors[.]com	NAMESILO, LLC
https://dayproud[.]us	hanproud[.]com	NAMESILO, LLC
https://hungarytoday[.]hu	hostwt[.]com	NAMESILO, LLC
https://www[.]newsteps[.]org	newstepsco[.]com	NAMECHEAP INC
https://www[.]bajaj[.]pe/english/finance	ovenfinance[.]com	NAMECHEAP INC
https://www[.]pharosjournal[.]com	pharaosjournal[.]com	NAMESILO, LLC
https://rghosts[.]com	rchosts[.]com	NAMESILO, LLC
https://schiebel[.]net	shebelnews[.]com	EPIK INC
https://money[.]cnn[.]com/data/us_markets	stockmarketon[.]com	NAMECHEAP INC
https://www[.]stonecrestonline[.]com	stonecrestnews[.]com	NAMECHEAP INC
news.sky[.]com	stsnews[.]com	NAMESILO, LLC
https://tacomaweekly[.]com	tacomanewspaper[.]com	DOMAINSOVERBOARD.COM LLC
https://onedrive[.]live[.]com	teachingdrive[.]com	NAMECHEAP INC
https://www[.]theadminzone[.]com	theadminforum[.]com	NAMECHEAP INC
https://www[.]t-mobilemoney[.]com/en/home[.]html	themobilecard[.]com	NAMECHEAP INC
https://www[.]theadminzone[.]com	thetravelerspledge[.]com	NAMESILO, LLC
https://www[.]bbc[.]com/news	trendignews[.]com	NAMECHEAP INC
https://homeoutlet[.]com	worldhomeoutlet[.]com	NAMECHEAP INC

LUNARREFLECTION Domains		
Location Domain	**X.509 Certificate Domain (Typosquat)**	**Registrar**
https://www[.]easycounter[.]com	bfilmnews[.]com	NAMESILO, LLC
https://dominican[.]news	dom-news[.]com	NAMECHEAP INC
https://ezdiy[.]com	exdiy[.]com	NAMESILO, LLC
https://midcitymessenger[.]com	midcitylanews[.]com	NAMECHEAP INC
https://mindsetsft[.]com	mindsetsoft[.]com	NAMESILO, LLC
https://www[.]newfordtech[.]com	news-techh[.]com	NAMECHEAP INC
https://atpflightschool[.]com	nextgencpe[.]com	NAMECHEAP INC
https://ecobale[.]com/about-ecobale	nordicmademedia[.]com	EPIK INC
https://petslifenews1[.]blogspot[.]com	petslifenews[.]com	NAMESILO, LLC
https://www[.]nasaproracing[.]com	proracingnews[.]com	NAMESILO, LLC
https://spaceheaterparts[.]com	spaceheaterpro[.]com	NAMECHEAP INC
https://www[.]newsanalytics[.]us	theanalyticsnews[.]com	NAMECHEAP INC
https://www[.]dailyworldnewsgazette[.]com	theworldnewsgazette[.]com	NAMECHEAP INC
https://www[.]delivery[.]com	userdelivery[.]com	NAMESILO, LLC

cs2modrewrite Domains		
Location Domain	**X.509 Certificate Domain (Typosquat)**	**Registrar**
https://www[.]google[.]com	api[.]pcocot[.]com	GODADDY.COM, LLC
https://blizzard[.]com	d2rwiki[.]net	NAMECHEAP
https://rsa[.]com	eu-elb-10[.]rsa[.]eu[.]com	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
https://www[.]vmware[.]com	eu-elb-11[.]carbonblack[.]eu[.]com	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
https://www[.]splunk[.]com	forward[.]splunk[.]eu[.]com	GANDI SAS
https://www[.]securedretail[.]com	glogln[.]com	NAMECHEAP INC
https://gfuel[.]com	hefuel[.]com	GODADDY.COM, LLC
https://heroesofthestorm[.]com	herosofthestorms[.]com	NAMECHEAP INC
https://www[.]ftc[.]gov[.]tw	mergers[.]ftclibrary-gov[.]com	GODADDY.COM, LLC
https://www[.]microsoft[.]com	mic[.]dnsrd[.]com	NAMESILO, LLC
https://www[.]onlinebusinessadvice[.]uk	onlinebusinessadviceuk[.]com	GODADDY.COM, LLC
https://code[.]jquery[.]com/jquery-3.6.0.js	quiz[.]stakeverflow[.]com	NAMECHEAP
https://www[.]financesolutionsuk[.]org[.]uk	ret[.]workman-alerts[.]co[.]uk	NAMECHEAP
https://www[.]microsoft[.]com	saab[.]dnset[.]com	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
https://google[.]com	support[.]starbulk[.]gr	N/A
https://tsubox[.]com	tsubux[.]com	NAMECHEAP INC
https://www[.]cia[.]gov	update[.]aviraoperations[.]com	CSC CORPORATE DOMAINS, INC.
https://www[.]windowsupdate[.]com	www[.]windowsupdate[.]com	NAMECHEAP INC
https://zincone[.]com	zinczone[.]com	NameSilo, LLC

Cobalt Strike samples affiliated with cs2modrewrite			
IP	**X.509 Certificate Domain (Typosquat)**	**File Hash**	**Referral Location**
139.99.178[.]56	midcitylanews[.]com	147991cd55a00ebb2f-fe8053e49f40d-13d334c54d073b083578bbbed-cd6b2389	midcitymessenger[.]com
139.99.178[.]56	midcitylanews[.]com	ffa980b2a4a88c68f62288de56e9cf-ccacbb3f738492f98dff-419c5f2f897377	midcitymessenger[.]com
103.232.53[.]230	dom-news[.]com	1. 92534b3d5e69c0be7dad0efed6b-5f0133ef00c0227a42853dc-62cc383ca747c5 2. 76975c897d6010e1faec-7c2c4cb4fbf3aa5b09c7cf80fc-8fa05831c2439db86a	dominican[.]news
139.99.167[.]177	cbdnewsandreviews.net	a4f1f09a2b9bc87de90891da6c0f-ca28e2f88fd67034648060cef9862a-f9a3bf	newsreview[.]com
45.179.89[.]37	hanproud[.]com	c4ff632696ec6e406388e1d-42421b3cd3b5f79dcb2d-f67e2022d961d5f5a9e78	N/A
195.206.181[.]169	tacomanewspaper[.]com	1f5a915e75ad96e-560cee3e24861cf6f8de299fd-f79e1829453defbfe2013239	tacomaweekly.]com
N/A	1. worldhomeoutlet[.]com 2. theyardservice[.]com	1. ee44c0692fd2ab2f01d17ca4b-58ca6c7f79388cbc681f885b-b17ec946514088c 2. ee42ddacbd202008bc-c1312e548e1d9ac670dd3d86c999606a3a01d464a2a330	N/A
159.65.184[.]99	glogln[.]com	43886ea4e57b421bb15bb-26f949ef3b1d9056229357b62babb-7fec56f7cd0975	securedretail[.]com
45.32.59[.]31	vmtoolsupdate[.]com	N/A	vmware[.]com
13.67.239[.]91	pcocot[.]com	1. 1b0318224a-1d139510139e-1765c5e7b1295fc-29c0ee861ea33a1ff-4f68a93023 2. fbd2233ff798f26fb-3998f5149af251f07fe-4fa06b255dd-6b991a569ae8097d5	google[.]com

COSMICNODE Hashes	
SHA256	**Filename**
6ee1e629494d7b5138386d98bd718b010ee774fe4a4c-9d0e069525408bb7b1f7	DeleteDateConnectionPosition.dll
3fcefd837ff32d28ccf3edb65954e595f8bdc06c9975e3cb46b71eefcf-1ca770	amber.exe
6473dbb511354618ff5dc332f9a0c035ba6f2699431e2d2e-766c830136afb64d	amber.exe
90fb7b856c0d34eaeca78e85a4ad5d699cff-6b4140a3514061068232a68bc95a	openvpn.exe
c6a3e82482d42b361d794bee779bff231082e15a7d2552093c46e-7136a2c00c5	amber.exe

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.