AWAKE

The Internet's New Arms Dealers:

Malicious Domain Registrars

AWAKE

The Internet's New Arms Dealers: Malicious Domain Registrars

Technical Summary

The Awake Security Threat Research Team has been tracking a massive global surveillance campaign that affects almost every enterprise we have investigated, making it the most successful and prevalent we have observed to-date. All related activity is tied to a single internet domain registrar: Gal Communication (CommuniGal) Ltd (GalComm).

Yes, we should say that again. We are not talking about a malicious domain "registrant," which is an end-user who utilizes the services of a domain "registrar" to obtain domains. In this report, we examine the behavior of a domain name registrar themselves – one of the relatively few organizations responsible for the management of the central registry database relied on by the entire internet.

As you will see in this report, this registrar, who also maintains a Registrar Accreditation Agreement with ICANN, is responsible for putting far more malicious domains, malware, and exploitative content on the internet than legitimate content. We believe the research and analysis summarized in this report proves that GalComm is at best complicit in malicious activity.

What Awake Security Found

- **Of the 26,079 reachable domains registered through GalComm, 15,160 domains, or almost 60%, are malicious or suspicious.** We also found and present evidence of these domains being used to host both traditional malware and browser-based surveillance tools. A list of these domains can be found here .
- In the past three months alone, we have **identified 111 malicious or fake Chrome extensions, downloaded approximately 33 million times**[1], that use GalComm domains for attacker command and control infrastructure as well as loader pages for the extensions. These extensions can take **screenshots, read the clipboard, harvest credential tokens stored in cookies or parameters, grab user keystrokes (like passwords)**, etc. A list of these Chrome extensions can be found here. Awake has since worked with Google to take down these extensions from the Chrome Web Store.
- After analyzing more than 100 networks across financial services, oil and gas, media and entertainment, healthcare and pharmaceuticals, retail, high-tech, higher education and government organizations Awake discovered that the actors behind these activities have established a **persistent foothold in almost every single network**.

Three notable aspects emerged during this investigation:

Evading Security Detection and Analysis

Domain categorization engines, online scanners, reputation checkers, and similar scanners used by security professionals have almost all the malicious domains labeled as "safe," "parked," etc. Therefore, most of the malicious activity is unidentified and appears to bypass enterprise security proxies, next generation anti-virus and other security controls. One reason for this appears to be a smart method for filtering/blocking requests used by this attack campaign. If the client is connecting to the domain from a broadband, cable, fiber, mobile, or similar fixed-line Internet Service Provider (ISP) type of network, then the client will be delivered the malicious payload. This allows all normal users and enterprises to pass through the filter. If the connection is coming from a data center, web hosting service, transit networks, VPN, or proxy, the request is redirected to a benign page.

Chrome Store Bypass

Some campaigns employed creative methods for getting extensions installed on endpoints and bypass the Chrome Store. They do so by loading a self-contained Chromium package instrumented with the malicious plugins. Because most users don't recognize the difference between Chrome and Chromium, when prompted to make the new browser their default, they frequently do – making their primary browser one which will happily continue to load malicious extensions from other GalComm related sources.

1 This represents total downloads for extensions that were live in the Chrome Web Store as of May 2020. As we point out in this report, many extensions were not in the Chrome Web Store in the first place.

Very Little Legitimate Traffic

To put it in context, GalComm accounts for an extraordinarily small percentage of domains on the internet. Compared to a common registrar like GoDaddy, it appears that GalComm has only 0.03% of the registrations as GoDaddy. When removing hits to malicious or suspicious domains, most networks observed had zero legitimate traffic to domains registered through GalComm.

The rest of this paper dives into the technical details in four chapters:

Chapter 1

discusses the campaigns uncovered by Awake including the use of malicious Chrome extensions

Chapter 2

covers connections between the threat we document in this report with traditional malware campaigns

Chapter 3

describes the techniques used by the attackers to evade detection

Chapter 4

addresses the GalComm connection and the wide-reaching threat posed by malicious domain registrars to the very underpinnings of the internet.

We end with the key implications and lessons this research surfaces for enterprise security teams.

Chapter 1
Browser Extensions: The New Rootkit

Chrome and other browser extensions represent a highly useful tactic for attackers since host-based security solutions tend to have difficulty in discerning legitimate from malicious activity when it is performed within the browser. This is especially problematic since most people conduct a significant part of their daily business activities within the browser. Rogue access to the browser therefore frequently means rogue access to the "keys to the kingdom"—from email and corporate file sharing to customer relationship management and financial databases.

Our research uncovered a total of 111 malicious Chrome extensions. Appendix B vprovides a list and includes extensions that were found to upload sensitive data or not perform the task they're advertised to perform (generally, they surveil user activity and device properties). Of those, 79 were available in the Chrome store as of the first week of May 2020 . As for the others, many of those have never been available in the Chrome Store and we examine a case study of this in Chapter 3.

Stealing Sensitive and Private Data

At first glance, the sleeper agent extensions appear to do nothing. We believe these are part of a more general trend where malicious actors are pushing malicious payloads to browser apps and extensions after the "clean" version has been approved.[2] In some cases, it is the threat actor themselves doing this work. In other cases, the app or extension developer later pushes malicious payloads for profit.[3]

As a case study, we present one of these extensions deceptively called "Management extension - Internal Chromium Extension." Figure 1 shows the permissions (capabilities) it has. As you will notice, it can collect what you type in the browser, tokens you receive from internal corporate sites (and of course public ones), access your clipboard, take screenshots, and harvest other extremely sensitive sources of information.

```
"description":
   "Management extension - Internal Chromium
Extension",
  "permissions": [
   "<all_urls>",
   "management",
   "background",
   "storage",
   "cookies",
   "tabs",
   "webRequest",
   "webRequestBlocking",
   "unlimitedStorage",
   "contextMenus",
   "bookmarks",
   "webNavigation",
   "history",
   "topSites",
   "activeTab",
   "alarms",
   "browsingData",
   "clipboardRead",
   "clipboardWrite",
   "contentSettings",
   "debugger",
   "declarativeContent",
   "desktopCapture",
   "downloads",
   "gcm",
   "geolocation",
   "identity",
   "idle",
   "nativeMessaging",
   "notifications",
   "pageCapture",
   "power",
   "printerProvider",
   "privacy",
   "proxy",
   "sessions",
   "system.cpu",
   "system.display",
   "system.memory",
   "system.storage",
   "tabCapture",
   "http://*/*",
   "https://*/*"
 ],
```

Figure 1: The permissions (or capabilities) of this browser extension gives it full access to almost anything a user or web page does or contains.

Tricking the Victim

The extensions we examine in this paper can be loaded onto victims in a variety of ways. Some involved false lures—professional-looking web pages like that shown in Figure 2 used to trick users into installing the malicious Chrome extensions. Others appear to be downloaded by previously installed adware, as recent research by TrendMicro[4] shows. Finally, as we examine in Chapter 3, some appeared to bypass the Chrome Web Store entirely.

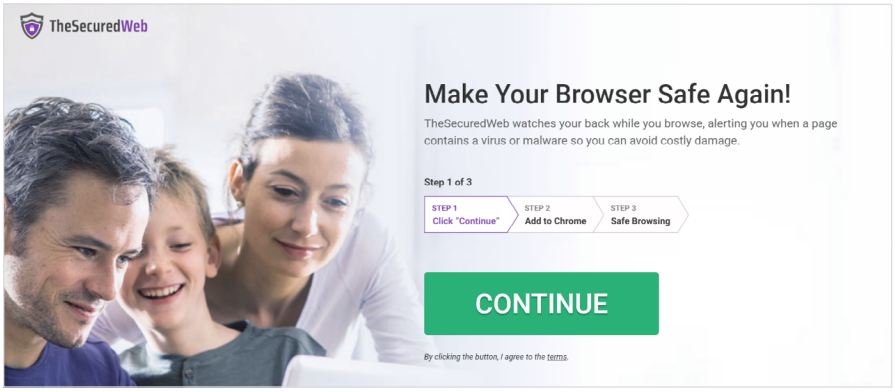


Figure 2: Lure to get the victim to install a malicious Chrome Extension

2 https://www.infosecurity-magazine.com/news/fiveyear-phantomlance-campaign/
3 https://medium.com/csis-techblog/installcapital-when-adware-becomes-pay-per-install-cyber-crime-15516249a451
4 https://blog.trendmicro.com/trendlabs-security-intelligence/exposing-modular-adware-how-dealply-iserik-and-managex-persist-in-systems/

As you might expect, the extensions themselves are frequently quite ineffective at the job they "promised" to do for the user. For instance, Figure 3 shows a visit to a page that is malicious. The security extension installed as part of one of the campaigns uncovered by this research is however perfectly happy with the page and its contents, giving it a "Secure" rating. After visiting many known-bad exploit sites, the extension reported them all as "Secure."

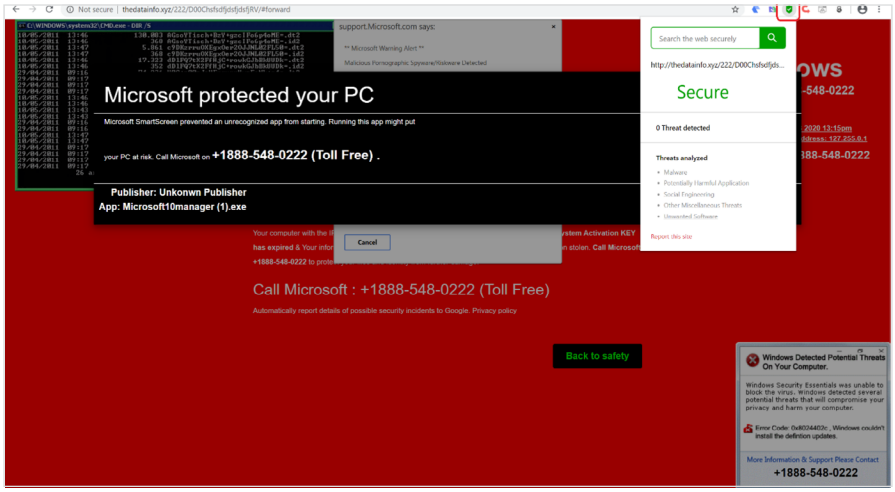


Figure 3: The extension shows every website as being "Secure," no matter what the website is trying to do. In other words, these extensions do indeed read your web page content, but not for the purposes of "security." It is worth noting that Awake researchers attempted to call the telephone number displayed, multiple times, but the calls were never answered.

Security experts can often visually identify fake or malicious extensions in the Chrome Web Store because:

- They tend to have a relatively large number of users, even though it's an unknown brand with little information about the company on the web.
- Further, whether few or many reviews are present, the reviews are generally great. If there are high numbers of users and high numbers of positive reviews, this can additionally indicate the user count has been artificially inflated with fake downloads (coupled with the fake reviews) in an effort to make the extension look more legitimate and get better placement in the store.

How Awake Discovered This Activity

About a year ago, Awake's Threat Research team developed an Adversarial Model (behavioral models for automated detection in Awake that can be easily created/copied/edited by analysts and users) allowing us to detect a large volume of malware that is missed by traditional tools. The model's basic function is to identify traffic using any protocol (known or unknown), that is:

- Going to a relatively rare destination for the observed network, and
- Seems to be uploading data, even small amounts, and
- The destination is not already known-good[S1], and
- Has been seen from the same device 3 of the past 7 days (or at least once a week for the past 3 weeks).

Awake's Adversarial Modeling Language (AML) is designed to be open and editable by any Awake user, meaning any user can create highly sophisticated statistical models (including leveraging Machine Learning). Because the language is open, you can see exactly how all our internal models work, and even create your own derivative models. A simplified version of the model referenced here looks like this:

```
workbench.db.persistenceBySourceDevice 3w 1w 3
(domain.number_associated_devices < 20 && recipes.flow.upload && recipes.destinations.domains.not_known_good)
```

This heuristic is looking for 1) signs of uploads, 2) in any known or unknown protocol, 3) going to a relatively rare destination, 4) that is not already known-good, and 5) where the activity is seen from the same source device at least once per week over the past three weeks. "3W 1W 3" means "look back 3 weeks, divide that time into 1-week buckets, and identify this activity at least once in each of those three buckets." Threat hunters use a variety of custom models like this in Awake to detect activity that is impossible to identify with traditional techniques and common ML methodologies.

As you may imagine, this model is extremely effective at catching a wide variety of malware. From traditional compiled executables, to fileless and scripted remote access – if it is persistent, it is easily discoverable this way.

On a related note, AML also helped uncover the malicious extensions found harvesting sensitive data from end-user workstations and exfiltrating it over TLS. Awake threat analysts were able to discover multiple such attempts at encrypted exfiltration using Awake adversarial models like this one:

```
(recipes.flow.subtle_upload.tls || recipes.flow.subtle_upload.http) && domain.registrar.name in [ "CommuniGal Communication Ltd.", "Gal Communication (CommuniGal) Ltd."]
```

S1 Filtering known-good is a double-edge sword. This can also filter certain types of traffic to Amazon, Azure, etc. Because of that, we have other specialized models that detect C2 to major cloud service providers with a high degree of accuracy.

- Finally, most of the time, these extensions are relatively new but still have very high numbers of users (see Figure 4). As we show through this research, a significant contributing factor to this "popularity" is the fact that the extension is involved in highly successful attack campaigns.

These are just a few of the "red flags" we used in connecting the threat dots across the Chrome Web Store.

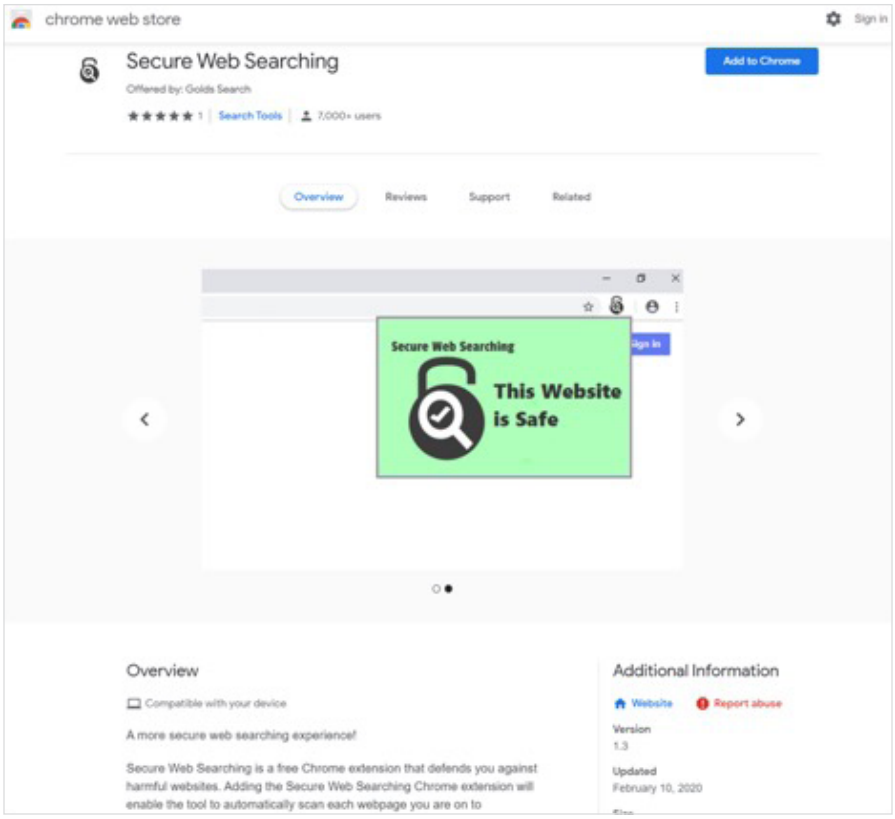


Figure 4: One of the many malicious browser extensions that doesn't do what it purports to. This one is only version 1.3, is not backed by a real company, yet has more than 7,000 users.

Figure 5 also puts this into context and compares popular extensions with the malicious ones uncovered by this research.

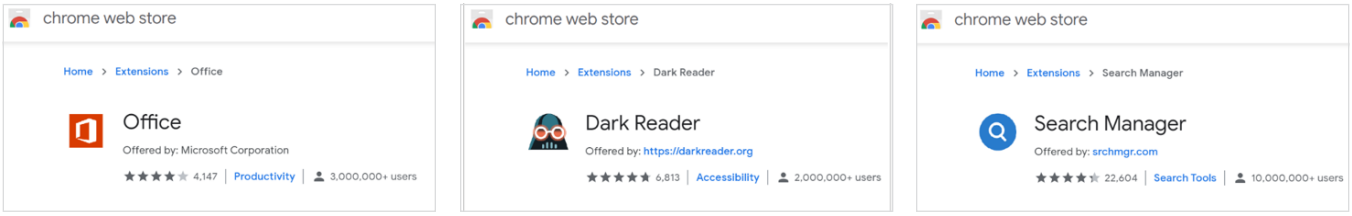


Figure 5: Here we see the official Office extension from Microsoft has 3M downloads and 4.1k reviews. Dark Reader, one of the most popular extensions of all-time has 2M downloads and 6.8k reviews. However, Search Manager, a GalComm-related extension, has over 10M downloads and 22.6k reviews! In addition to artificial downloads associated with the fake reviews, this number also illustrates the success of these campaigns.

Awake researchers also observed many extensions were added multiple times to the store, with only superficial variations between each new addition to the store. For each of the three screenshots in Figure 6, notice that each of these "different" extensions (respectively, gfcmbgjehfhemioddkpcipehdfnjmief, clopbiaijcfolfmjebjinippgmdkkppj, and lpajppfbbiafpmbeomp-binpigbemekcg) have the same artifacts, including:

- The same graphic where only the main color changes.
- The same version of 10.1.4.*.
- The same descriptive text in the overview.
- The same, or close to the same size (there are many more examples like this, and the size is largely constant across all samples).
- Very high numbers of users, given the purpose of the extension.

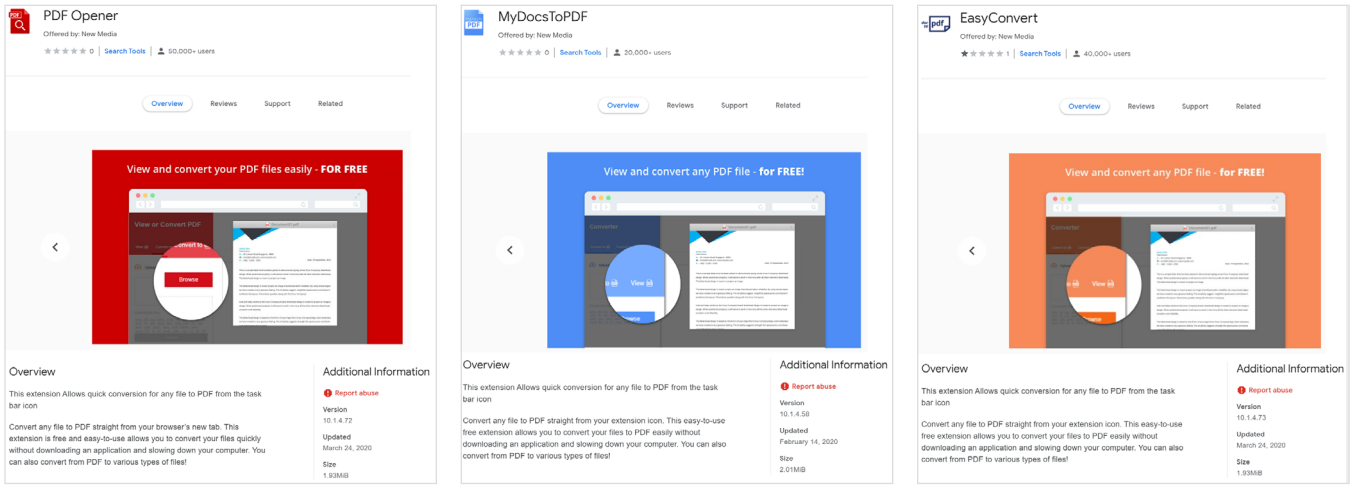


Figure 6: The descriptive overview text, version numbers, graphics used, and size are basically the same in these screenshots, along with the 10 other supposedly different PDF converters sharing these same artifacts.

It is also interesting to note that the "security" themed extensions as displayed in Figure 7 are some of the most overinflated extensions with fake reviews. This is especially significant since our research showed that these extensions appeared to be the most egregious in stealing sensitive information, making them clearly the highest risk among the in-store extensions.

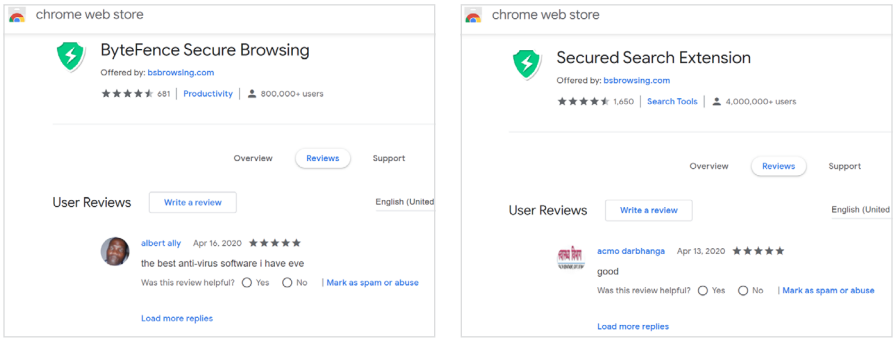


Figure 7: The security-related extensions typically had hundreds to thousands of fake reviews. These extensions appeared to be the worst offenders exfiltrating significant amounts of sensitive data including all searches performed, pages visited, URLs (usually containing internal enterprise webapp tokens and related information), web page content, etc.

Although ByteFence is supposed to be nothing more than a rebranded version of Reason Core Security, multiple people have experienced this extension downloading malware as well, including as recently as April 2020 (Figure 8).[5] We have also found it bundled with malware in-the-wild during this investigation.

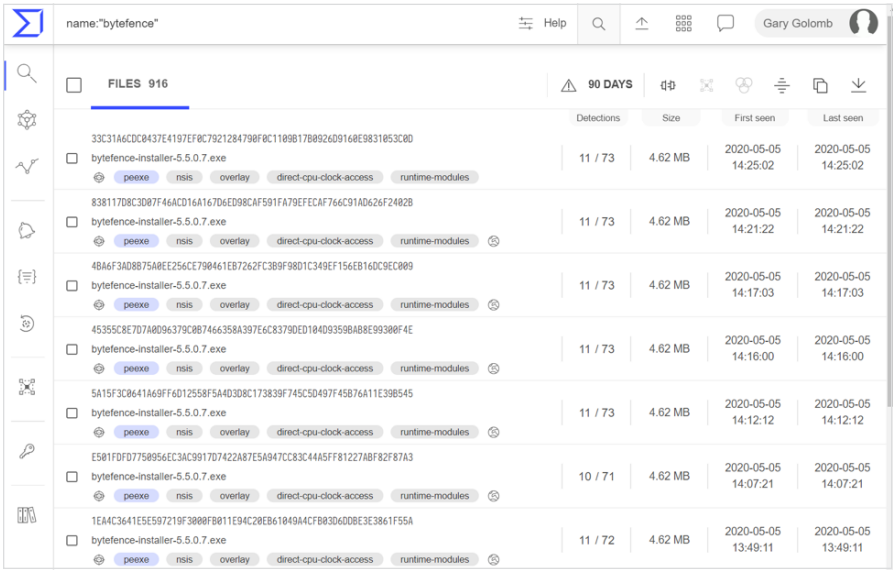


Figure 8: VirusTotal receives a very large number of malicious ByteFence binaries, per day. This figure shows about 1-hour of submissions to VirusTotal.

5 https://malwaretips.com/threads/ever-heard-of-bytefence.56677/post-543222

In all, if we examine only the extensions with surveillance-like capabilities–that is, the extensions which advertise one function (like security) but actually do nothing other than send information about the endpoint or user-activities to GalComm-registered domains—then we find there have been **32,962,951 downloads of these extensions**. While this number likely includes artificial downloads as described earlier, we believe the actual number of endpoints with these extensions is not substantially less, and quite likely more. This is based on a combination of:

- The approximately 33 million downloads account only for extensions live in the Chrome Web Store at the beginning of May 2020.
- However, only about half the extensions we document in Appendix B are in the store. The other half, while many are still currently active, have been loaded on endpoints in ways that bypass the Chrome store completely (as described in Chapter 3), making it difficult to get an install count for those.

Clearly the dependence on the browser for modern computing when combined with the pervasive nature of these malicious extensions makes for a potent tool for deep surveillance and data theft.

Chapter 2
The Absurd Line Between Espionage-Level Malware and PUPs

As our investigation progressed, another insidious angle emerged. The same domains we identified as malicious and tied to the Chrome Extensions appeared to be connected to other campaigns as well. We believe this connection is not a coincidence. In fact, just in the past two years, we have seen a ramp up of the use of surveillance style tools as part of larger nation-state campaigns. For instance[6]:

- Ocean Lotus, an espionage group believed to be State sponsored and operating out of Vietnam (first made notorious by their stealthy use of JavaScript implanted in websites to quietly track and profile visitors of compromised sites), has now evolved to distributing fake apps with elaborately concocted cover stories through legitimate app stores. (Like the examples in Chapter 1.)

- The Pakistani government[7], military, and other officials have been the target of sophisticated espionage campaigns based on fake apps and elaborate phishing schemes.

- Espionage groups like Confucius have distributed real, functional, and mostly benign applications – such as chat apps that only begin surveillance functions (e.g. collecting SMS messages, contacts, etc.) after special keywords of interest have been used in chat.[8] This is not a far-cry from extensions that convert PDFs to Office documents (and vice-versa), especially when those files are being sent to unreputable remote servers to handle document collection and conversion functions.

Only a decade ago, the term "spyware" was most commonly associated with advertising programs, also known as "Potentially Unwanted Programs" (PUPs).[9] Today, spyware might be commonly associated with actual spying. This problem likely does not rest on the shoulders of security analysts across enterprises who are too resource-constricted to respond to PUPs/spyware detections. The problem, we believe, lies with the security products that label a very, very wide range of activity as PUPs/spyware these days. Consequently, security analysts across enterprises, often inundated to begin with, fail to respond to PUPs/spyware alerts that are frequently much more sinister than the labeling would have you believe.

Let's unpack an example of this and see how this connects to the broader surveillance campaign we have uncovered in this research report.

An In-The-Wild Case Study

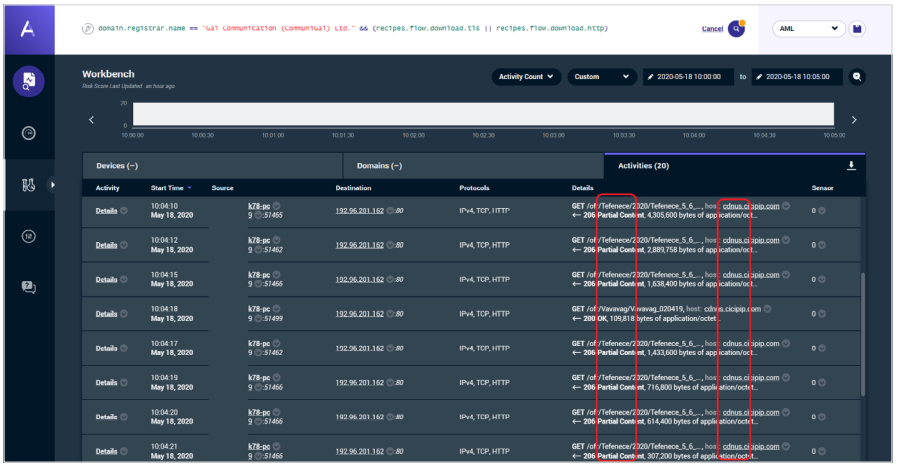


Figure 9: PUP content download from suspect / malicious domains identified in this report

In Figure 9, you see downloads of PUP content from the domains identified as suspect / malicious in our research. The IOCs in the red boxes (Tefenece and cdnus.*) are associated with a particular version of software discovered in mid-2017 that was classified as a PUP by security products.[10] (There is one noticeable difference seen in the example activity captured in Figure 9, which is the use of "2020" in the path, presumably indicating a new campaign for this year, 2020.)

6 https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html
7 https://apnews.com/eb3e1a9736fc48bdb223298340c14051
8 https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/
9 https://en.wikipedia.org/wiki/Potentially_unwanted_program
10 https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/pua_vitalia.ga

The subdomain IOCs “cdnus.*” and “cdneu.*” (not pictured in Figure 9, but also observed) are used by software known as InstallCore. In our analysis, InstallCore appears to be the second most used software to download files,[14] upload data, and communicate with the suspect / malicious domains identified in this report. The only software used more prolifically are Chrome Extensions.

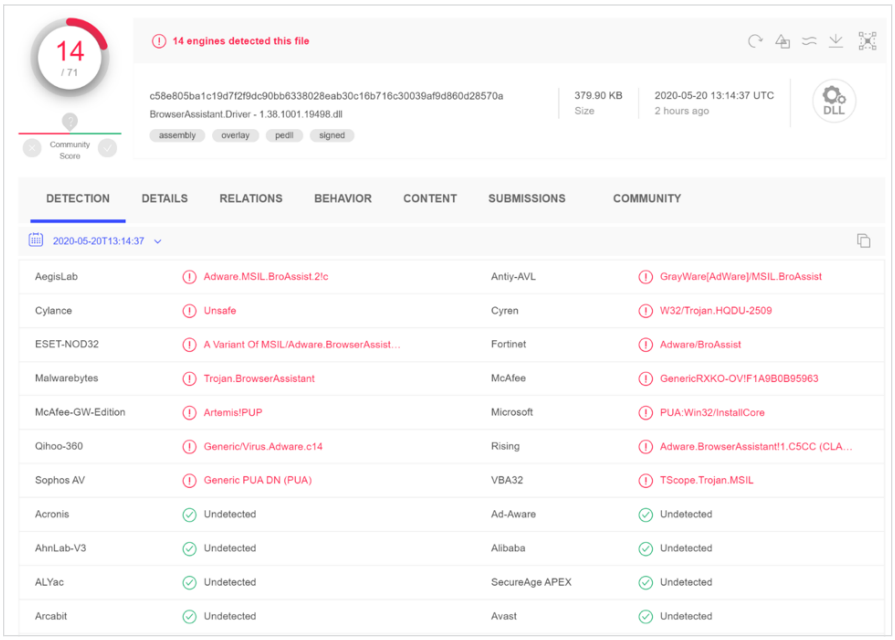


Figure 10: InstallCore generally has a relatively low detection rate and is usually labeled as a PUP or Adware.

InstallCore is owned by IronSource, both Israeli companies previously accused by influential researchers of fueling their businesses from malware.[11] InstallCore detection across security products is generally low, and most commonly it is labeled as a PUP or Adware. However, should this be the case? InstallCore’s business is based on Pay-Per-Install and it is frequently found to install later stage malware.[12]

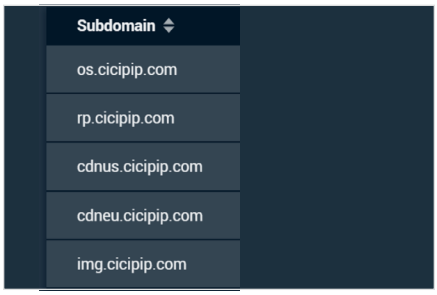


Figure 11: The subdomains in the observed network traffic that match InstallCore IOCs.

These are several connections to InstallCore and notable behaviors in our observed traffic. As identified previously, InstallCore frequently uses the subdomains cdnus.* and cdneu.*, but there are several other subdomains commonly used by the tool[13], all of which are seen in the network activity tied to the domains in this report.

We have been tracking behaviors associated with InstallCore activity in the wild through HTTP header fingerprinting. Most recently, however, the traffic patterns appear to show anomalies from the historical trend.

```
230 Bytes Starting 2020-05-18 10:04:08:702364000
HEAD /ofr/Tefenece/2020/Tefenece_5_6_4_0_170520 HTTP/1.1
Accept: */*
Host: cdnus.cicipip.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache
```

Figure 12: Sample request #1. Subdomain and URL artifacts here are associated with InstallCore.

```
166 Bytes Starting 2020-05-18 10:04:17:614361000
HEAD /ofr/Vavavag/Vavavag_020419 HTTP/1.1
Host: cdnus.cicipip.com
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
```

Figure 13: Sample request #2, made nine seconds after request #1. Again, the subdomain and URL artifacts are known to be associated with InstallCore.

11 https://www.businessinsider.com/ironsource-denies-its-for-malware-2015-3
12 https://blog.infostruction.com/2018/10/26/adware-empire-ironsource-and-installcore/
13 https://blog.infostruction.com/wp-content/uploads/2018/10/Ironsource-Domains-.txt
14 https://www.secureworks.com/blog/malware-lingers-with-bits

If you look closely at Figures 12 and 13, you'll see behavior that is rare for a single piece of software.

First, we see the use of the HTTP method "HEAD," which is used to check for the presence of a resource before requesting it. This superfluous step is not performed by most common applications, including web browsers. This artifact tells us that, while the User-Agent string is purporting to be Internet Explorer 11, it is not a web browser. This means we're not dealing with a browser plugin, but rather a stand-alone executable that, as evidenced by the requests over time, has established persistence on the device.

The most common occurrence of the HEAD method observed on the network, for Windows devices such as these, occurs when the Microsoft Background Intelligent Transfer Service (BITS) has been co-opted to download files.[14] However, when BITS is used, the HTTP headers are different from what we see in Figures 12 and 13. This seems to indicate that we're dealing with a stand-alone executable using custom headers that has established persistence on the device. Given that the HTTP fingerprints observed here are exceedingly uncommon in any of the environments we researched, we conclude that this standalone executable is itself rare. The "HTTP Fingerprints" we're referring to are the specific key:value pairs in the header, as well as the order of those pairs.

This leads us to another peculiarity about this traffic. The HTTP fingerprints themselves are different between Figures 12 and 13. This sort of behavior is generally only seen when two different software applications are making two different requests. Moreover, this pattern was observed consistently over time, so simple randomization of headers can be ruled out. Instead, this consistent but unique pattern we believe points to a single application making requests using two different configurations. In fact, we observed custom headers used not just for malware downloads and command and control (C2) but also for encrypted data exfiltration (Figure 14 and 15).

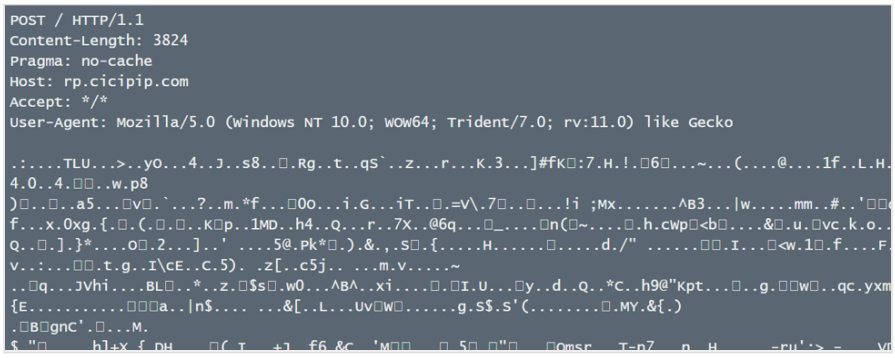


Figure 14: Devices uploading data to malicious / suspect domains.

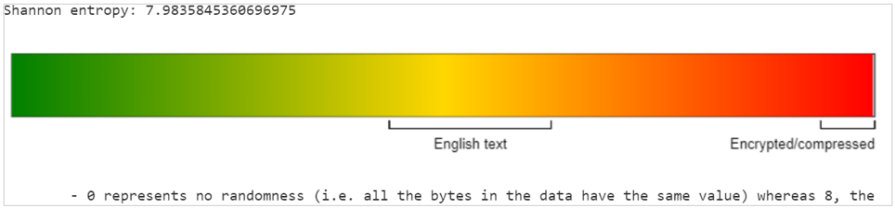


Figure 15: The entropy of the data uploaded (and downloaded) is extremely high at 7.98, which is close to maximum.

The Labels "PUP" and "Adware" Are Dangerous and Gross Misnomers

In Figure 14 and 15 we see the device uploading high entropy data. During our analysis, we were unable to inflate the data, meaning the data is likely encrypted as opposed to only compressed. Similarly, attempting to brute force the encryption yielded no luck, indicating that the encryption is more well-implemented than typical PUP applications. The TTPs observed for the software in this section include:

- Persistent encrypted uploads.
- Encrypted downloads, with sizes typical of malware executables.
- All communications with domains identified as malicious / suspect domains in this report.
- HTTP header artifacts pointing to custom and purpose-built software.

When we combine the TTPs just described with the IOCs examined earlier, then search for executables with the same TTPs and IOCs, we only find executables with the following behaviors (all close variations of[15] or[16]):

- Creates/installs a DirectInput object[17] and raw input device[18], commonly used by keystroke loggers.
- Drops files that have been identified as malware or associated with malware.
- Uses very long obfuscated CLI commands, a feature that is rare except for in malware.
- Tries to detect if it's running in a virtual machine.
- Checking for the presence of antivirus programs on the device.
- Contains several sandbox evasion techniques.
- Checks for kernel debuggers.
- Enables debug privileges.
- Actively tries to harvest browser history and cookies.

The activity performed by this software is the activity security analysts consider "malware," yet stunningly, these samples are labeled as PUPs, Adware, or Greyware by most antivirus products[19] (if detected at all), causing security teams to drastically miscalculate the risk faced by the enterprise. Frequently, security teams think of PUPs/Adware as the type of apps that annoyingly popup coupons, and many times security teams do not remediate PUP detections because of resource constraints. This is a dangerous strategy. "PUP" seems to have become a catch-all detection over the years, meaning full-fledged malware frequently ends-up with that label these days.

15 https://www.joesandbox.com/analysis/116664/0/html
16 https://www.joesandbox.com/analysis/152629/0/html
17 https://wikileaks.org/ciav7p1/cms/page_3375220.html
18 https://www.codeproject.com/articles/297312/minimal-key-logger-using-rawinput
19 https://www.virustotal.com/gui/file/dd335ad5fc927d8e109a50db93500020cd3290d587ca75e1a77bc6109369d191/detection

Chapter 3
Evading Threat Detection

It's interesting to note that almost all the campaigns uncovered as part of this threat research employed a variety of evasive techniques to prevent detection as well as complicate security analysis.

Tricking Security Analysis Tools

In most cases, the domains identified in this research appear to be very particular about the network the victim is making a request from. Not only are VPN and proxied connections redirected to benign landing pages, they also appeared to be filtering connections from data centers, web hosting services, and transit networks (Figure 16). The effect is that **all tested online website scanners, sandboxes, and reputation databases have these domains labeled as "safe"** (or a related label) **because they are redirected to benign parking pages, as their requests originate from data centers.**

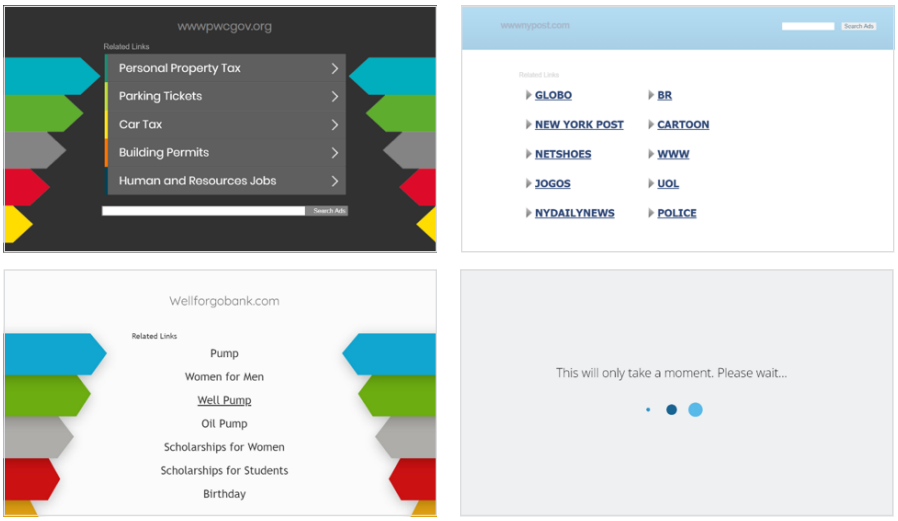


Figure 16: Four samples of pages returned by the malicious domains when filtering requests from VPN, proxies, data centers, web hosting services and transit networks. As a consequence security researchers and domain categorization engines incorrectly label these as "parked domains," when in actuality, only filtered requests get a parked page.

On the other hand, when connecting to the domain from a broadband, cable, fiber, mobile, or similar fixed-line ISP type of network, the client is directed to the malicious landing page. This allows "normal" users and enterprises to be exploited.

Let us look at one example of a malicious domain uncovered by this research: yougetsingal[.]com When visited through an anonymous proxy, the page shown in Figure 17 is returned. This is also the page returned when scanning the domain from an online security scanner or domain reputation checker (Figure 18).

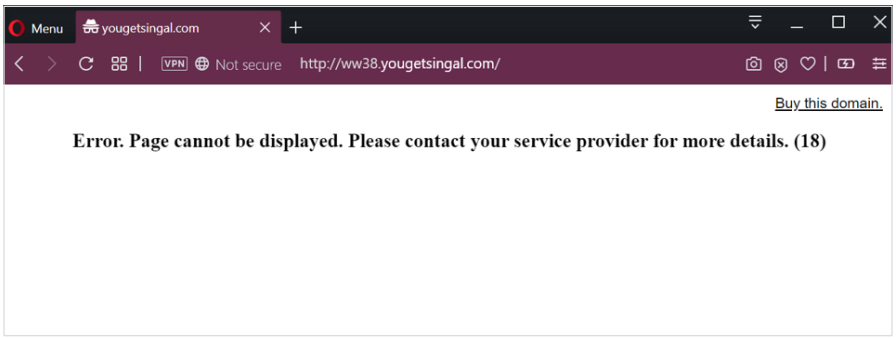


Figure 17: The page returned when visiting yougetsingal[.]com from behind an anonymous proxy.

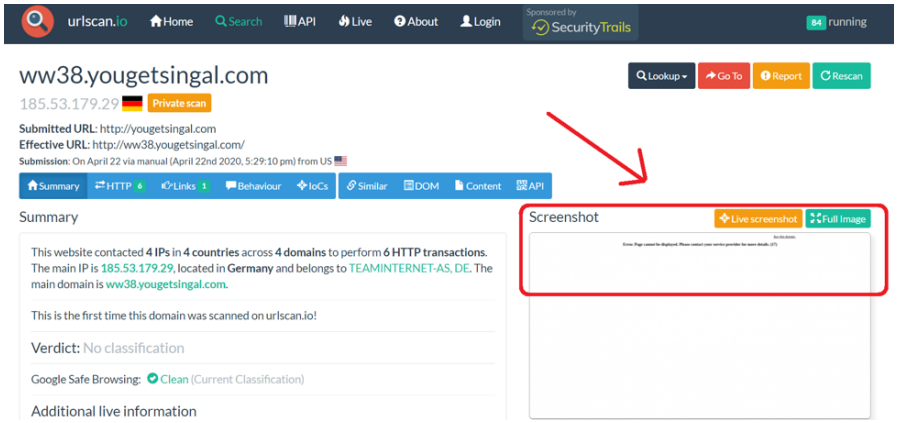


Figure 18: Online scanners and reputation checkers also get the same benign landing page. Cached result at https://urlscan.io/screenshots/19bc7acf-c7d9-4565-94d2-4ecef66ae0dc.png

In addition, our research also discovered the "benign" version of the landing pages change over time, as Figure 19 shows.

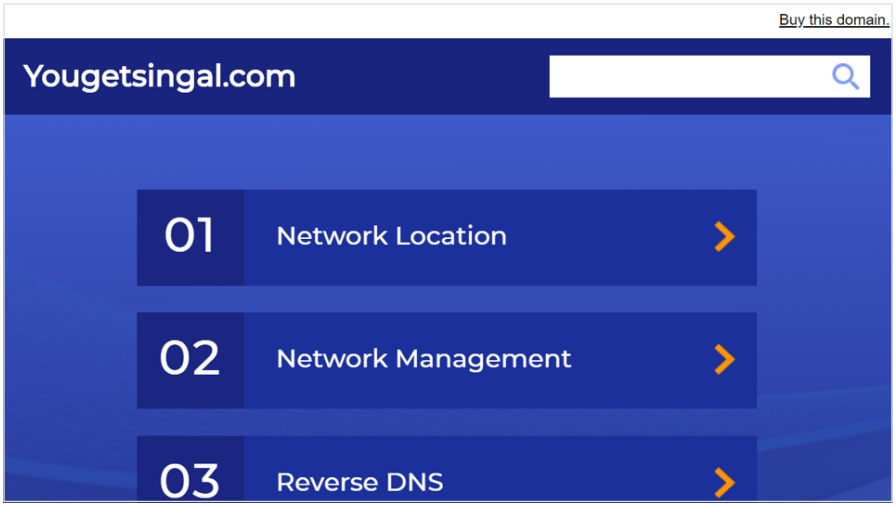


Figure 19: An interesting artifact of many of these campaigns is that the parked/benign page returned to a client will change. For instance, a filtered request for yougetsingal[.]com made a few hours later, provides a very different page from that shown in Figure 17.

However, if the user is coming from an enterprise or ISP-like connection to the internet, then they are directed to a malicious landing page with a lure intended to compromise their device (Figure 20).

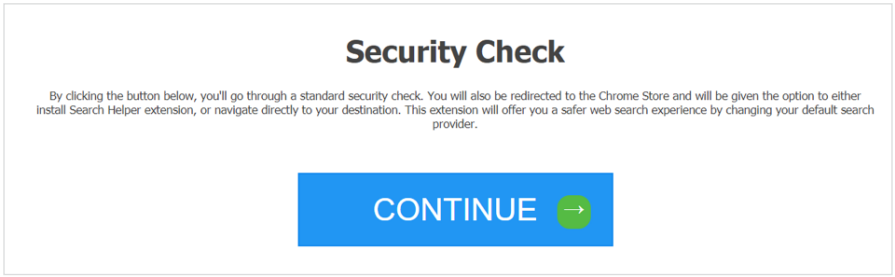


Figure 20: When the user visits the domain yougetsingal[.]com comes from a broadband, cable, fiber, mobile, or a fixed-line ISP type of network, the client is redirected to one of a variety of other types of malicious landing pages.

Figure 21 shows another example, more in the flavor of support fraud, that is presented to the victim.

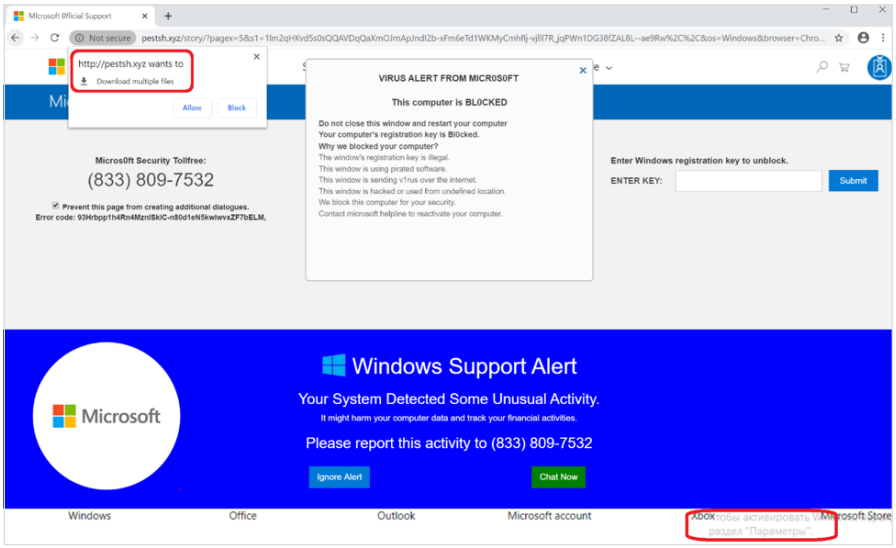


Figure 21: Another example of a malicious page returned when visiting the domain from an enterprise network or normal Internet Service Provider. Also notice the page is attempting to download multiple files to the computer.

Bypassing the Chrome Web Store

Recently, the Awake team discovered these campaigns utilize another evasive mechanism. Frequently, a custom version of a self-contained Chromium package is installed with malicious extensions already included. This technique allows the attacker to bypass the Chrome store completely and evade any security controls there. Additionally, many users unwittingly default to the new rogue browser when prompted at first run.

These rogue browsers appeared to have been installed by existing potentially unwanted programs (PUPs) already present on the victim system. This is very effective since the rogue browsers are self-contained, meaning other than the ability to just execute a program locally, very few other permissions are necessary.

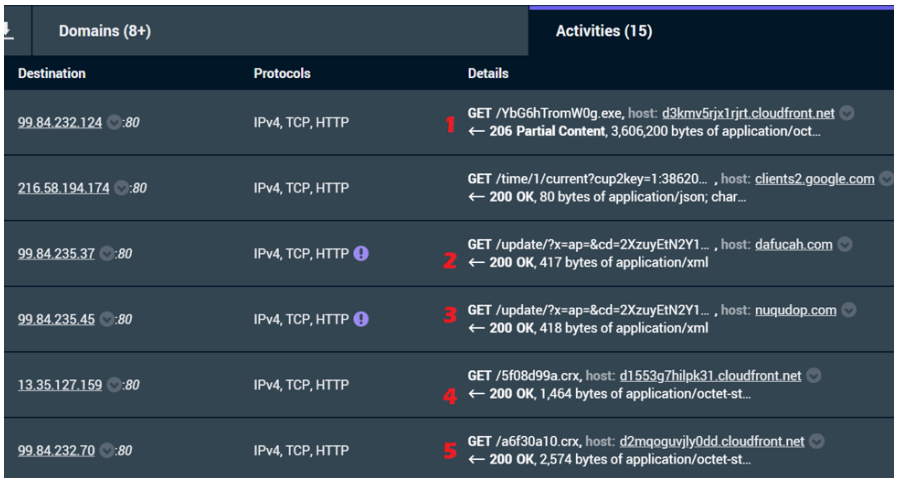


Figure 22: An already-installed PUP is seen downloading a patched (malicious) Chromium browser, thereby bypassing the Chrome store and any chance of public scrutiny for the extensions.

Figure 22 presents an example of this, as observed in the wild.

In this case, we observe the following network activities:

1) This is a request made by a previously installed but "sleeping" PUP. Using Awake's full packet capture capabilities we examined the contents of the session and observed the characteristic artifacts of an InstallCore request. Here, we see a request for the file YbG6hTromW0g.exe to the server d3kmv5rjx1rjrt.cloudfront.net.

2 & 3) These requests download a configuration file for the extension that is preinstalled with the browser.

4 & 5) Based on the configuration files received in #2 and #3, new requests are made to download additional malicious Chrome extensions. This allows the initial extension to evade detection by providing only a minimal set of loader-related features.

Normally Chrome is configured to only install extensions from the Chrome Store. However, by using a specially patched version of Chromium that happily accepts whatever extension it is directed to install, the attacker can bypass that control. Furthermore, extensions downloaded from CloudFront, a reputable hosting provider, are far more likely to be ignored by analysts than extensions downloaded from the domain in step 2: dafucah[.]com.

Other Evasive Techniques

The attackers also used other techniques to defeat security analysis. For instance, many of the domains implemented strict rate-limiting—i.e. if several requests are made, the client is redirected to one of the benign landing pages. Other examples implement server-side access control rules, such as the example in Figure 23, which only allows requests from one of the malicious browser extensions.

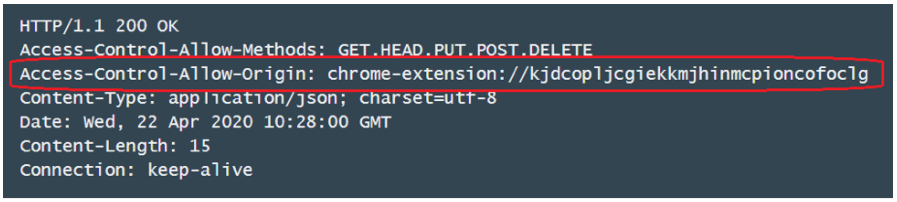


Figure 23: While server-side filtering of requests is more frequently done by IP address, searching through Awake's full packet capture database found some of the associated campaigns implement Access-Control-Allow-Origin[20] rules on the web server to ensure requests are made only from expected (malicious) Chrome extensions.

The variety of techniques above show that the threat actor behind these campaigns has gone out of their way to avoid detection and has been innovative (and effective) in their approach to quietly target and persist within victim networks.

20 https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Origin

Chapter 4:
The GalComm Connection

Throughout our research, we uncovered domains used for hosting malicious Chrome extensions, exfiltrating data, command and control, etc. All of these domains had something in common: they were all registered through a particular registrar: GalComm or Gal Communication (CommuniGal) Ltd (as shown in WHOIS). In fact, in 2019 , our threat researchers noticed that GalComm was becoming a common thread in our interactions with our customers. Since then, our analysis shows that almost 60% of the domains we have observed registered with this registrar are high risk for organizations.

For this report, we audited 26,079 domains registered by GalComm, as of early 2020. The analysis started with the characteristics of traffic profiles and patterns Awake has been observing in our customer networks over time. Additionally, we looked for patterns of how clients are redirected to various exploitation and landing pages, Finally, we focused on grouping by the malicious Chrome extensions observed in the wild, that relied on these domains. The investigation then expanded to include analysis of code used in pages served to clients, as well as an analysis of the mechanism employed by the domains to evade detection, detailed in Chapter 3.

All totaled, Awake observed 15,160 unique suspect or malicious domains. It's worth noting that many of these domains have been "hijacked," meaning they were registered using GalComm immediately after they expired. In fact, most of the reviews about GalComm on the internet are complaints about hijacked domains. This gives the attacker an advantage by defeating detection mechanisms looking for "newly created" domains.

Based on a variety of data points including those listed below, Awake researchers were able to categorize and cluster the domains and the associated attack campaigns as shown in Table 1 and Figure 24.

1) Download source for malcode, C2 server, or exploitive landing page.

2) JavaScript code used in pages returned to the client, including the number of scripts and characteristics of each script.

3).HTML elements used in pages returned to the client.

4) Server versions and types.

5) Return codes given to different types of requests and types of data/information returned with a given return code.

6) When errors were returned, the structure of error messages returned.

7) Where the domain is hosted.

8) Nameserver characteristics for the domain.

9) When the domain was registered by GalComm combined with registration information that may have existed before the GalComm registration (indicative of "hijacked" domain).

10) Redirection chain characteristics, in cases where clients are redirected to exploitative landing pages.

- **A)** In cases of redirects, we analyzed the number of servers in the redirect chain, how the redirection was performed, and characteristics of those servers as well.

11) Tracking and web analytics elements used in pages.

12) Characteristics of cookies used by the servers.

In addition, as Awake researchers considered the risk these campaigns pose to organizations, the following guidelines were used:

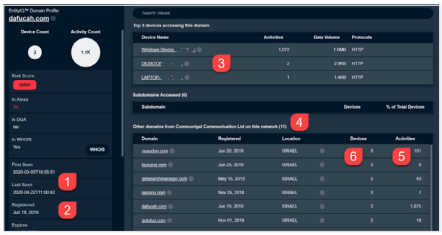
High	High/Medium	Medium	Medium/Low
Direct and/or recent activity leading users to exploitative pages, hosting malcode, or serving as C2 for malicious or surveillance code observed.	Significant overlap with C2 TTPs and a lack of legitimate artifacts but no recent C2 activity observed in the wild.	Contains references to code used within High and High/Medium domains but no redirection was being performed.	Utilizes the parked domain monetization tactics seen with High, High/Medium or Medium domains but no redirects observed.

Table 1: Categorization of Malicious and Suspect GalComm Domains

Category	Number of Domains	Risk Label
Campaign A Loader	797	High
Dormant Campaign A TTPs	1,433	High
Campaign B Loader	3,294	High
Campaign C Loader	1,388	High
Mal Loader TTPs (80%) + Redirects (20%)	2,969	High
Browser Extension C2	259	High
Overlap TTPs: Protected C2 and Shady Ad Network	319	High/Medium
Dormant Loaders	2,290	Medium
Parked Domain Monetization	2,411	Medium/Low

This report does not attribute specific actors to each of these campaigns. They could be the same or different actors. However, because of how the characteristics of each varied, we assess with high confidence that these are separate campaigns.

Most discoveries are not preceded by, "Eureka!" But rather, "Hmmm. That's strange …"



We first noticed these related campaigns about a year ago. As we began uncovering this persistent traffic across networks, we also noticed something strange in the information presented to our analysts by the platform, as shown below.

Awake's EntityIQ Domain Profiles answer common questions analysts have about the destinations for enterprise traffic. Here we see the analytics have automatically identified the domain as high risk, and additionally is showing the user other domains seen on the network from the same registrar.

The Awake platform precomputes answers to investigators' most common questions, even if they forget to ask. For example, when malicious activity is detected on a network (by either automated detection or hunting), an investigator might need to answer questions like:

1 How long has the domain been in our network?

2 Where was the domain registered?

3 What other devices on our network are accessing the same domain?

4 How common is the registrar?

5 What other traffic in my network is going to domains from the same registrar?

6 How many other devices in the network are going to domains from the same registrar?

There are powerful questions that can quickly turn a simple alert into a far-reaching campaign investigation.

As you can see above in the screenshot, the answers to the following questions have been precomputed for the analyst, without requiring them to remember to search elsewhere for answers:

Q How long has the domain been in our network?
A About six weeks at the time of this screenshot.

Q Where was the domain registered?
A Israel.

Q How common is the registrar?
A Not very common at all. Overall time and traffic, very few domains have been seen associated with this registrar.

Q What other traffic in my network is going to domains from the same registrar?
A A handful of those domains have dozens of activities associated with them, meaning they are potentially persistent C2 domains too.

Q How many other devices in the network are going to domains from the same registrar?
A Three. Based on the information precompiled for the analyst, it appears the three devices are all exhibiting the same behavior and trying to communicate with the same set of domains from this registrar.

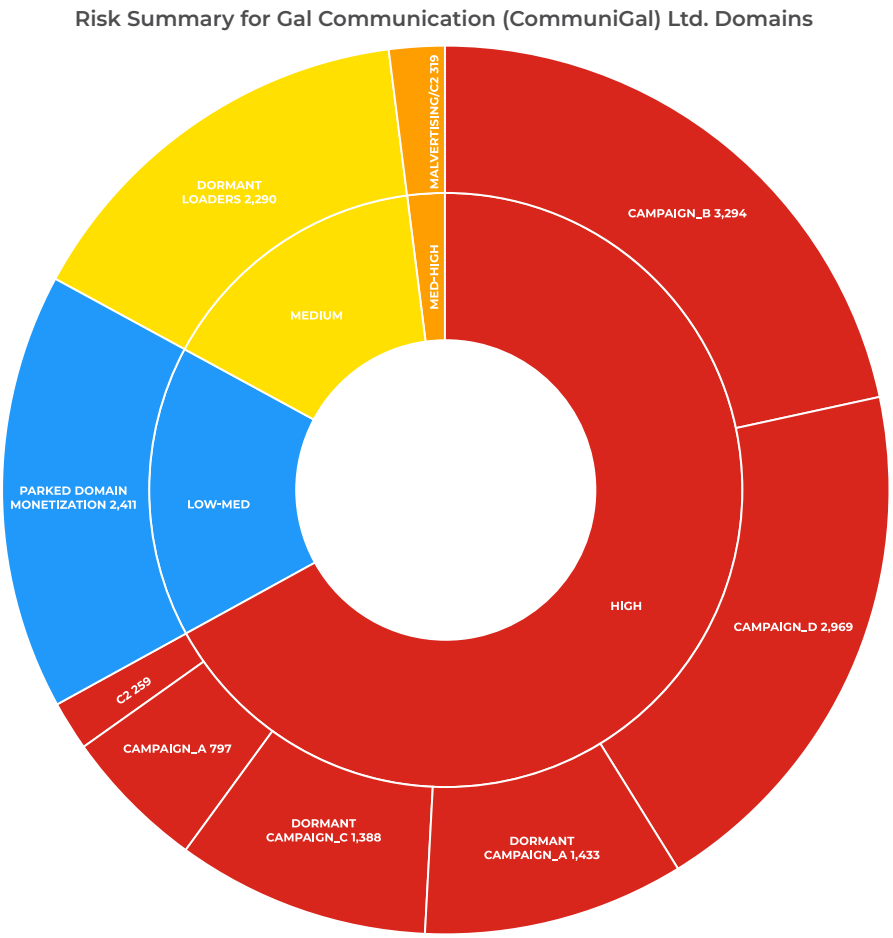


Figure 24: Distribution of GalComm-associated domains tied to malicious or suspicious activities.

In fact, the connection to GalComm goes deeper. For instance, if we look for the customized version of Chromium described in Chapter 3 by either name or hash, the search yields almost no results as shown in Figures 25 and 26.

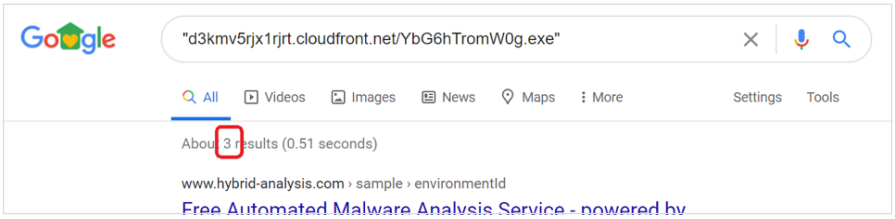


Figure 25: Only three Google results found when searching for the file by URL

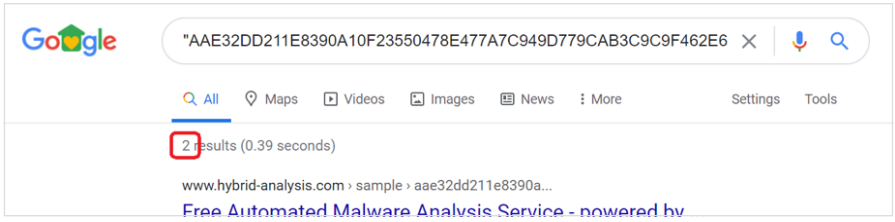


Figure 26: Only two Google results when searching for the file by hash.

However, hybrid-analysis.com has made a very interesting connection:

The only known locations this file has been downloaded from is the CloudFront resource described in Chapter 3 (Figure 22), and a GalComm registered domain—bwnbr[.]com. Based on Awake's analysis of the TTPs associated with this domain, we assess with high confidence that it belongs to a small cluster of 18 GalComm registered domains. When allowing for slight variations in TTPs, this cluster is closely related to another cluster of 134 domains. Both lists are provided in Appendix C.

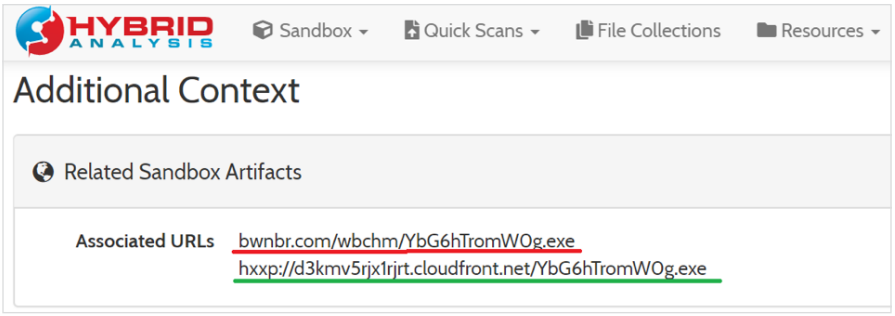
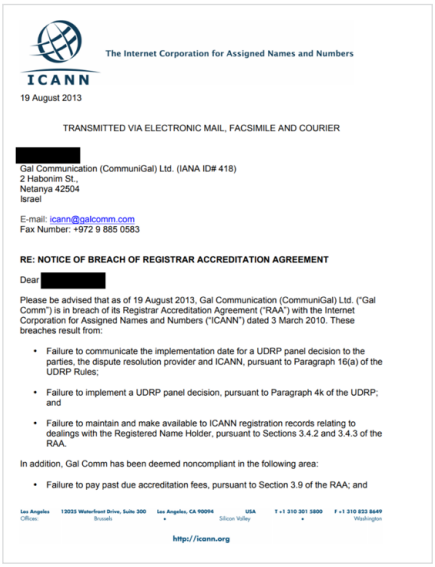


Figure 27: There are the only two known locations the custom Chromium version has been downloaded from (hashes are the same at both locations). One is the CloudFront resource we examined in Chapter 3 (Figure 15) while the other is a GalComm domain.



The Internet Corporation for Assigned Names and Numbers

ICANN

19 August 2013

TRANSMITTED VIA ELECTRONIC MAIL, FACSIMILE AND COURIER

[redacted]
Gal Communication (CommuniGal) Ltd. (IANA ID# 418)
2 Habonim St.,
Netanya 42504
Israel

E-mail: icann@galcomm.com
Fax Number: +972 9 885 0583

RE: NOTICE OF BREACH OF REGISTRAR ACCREDITATION AGREEMENT

Dear [redacted]

Please be advised that as of 19 August 2013, Gal Communication (CommuniGal) Ltd. ("Gal Comm") is in breach of its Registrar Accreditation Agreement ("RAA") with the Internet Corporation for Assigned Names and Numbers ("ICANN") dated 3 March 2010. These breaches result from:

- Failure to communicate the implementation date for a UDRP panel decision to the parties, the dispute resolution provider and ICANN, pursuant to Paragraph 16(a) of the UDRP Rules;
- Failure to implement a UDRP panel decision, pursuant to Paragraph 4k of the UDRP; and
- Failure to maintain and make available to ICANN registration records relating to dealings with the Registered Name Holder, pursuant to Sections 3.4.2 and 3.4.3 of the RAA.

In addition, Gal Comm has been deemed noncompliant in the following area:

- Failure to pay past due accreditation fees, pursuant to Section 3.9 of the RAA; and

Los Angeles Offices: 13333 Waterfront Drive, Suite 300 Los Angeles, CA 90094 USA T +1 310 301 5800 F +1 310 823 8649
Brussels • Silicon Valley • Washington

http://icann.org

Figure 28: GalComm breach of ICANN agreement. https://www.icann.org/en/system/files/correspondence/serad-to-fogel-19aug13-en.pdf

So, who is GalComm?

As it turns out, the answer to that question is not-so-easy to obtain. When performing a Google search for GalComm, the first result is a NOTICE OF BREACH OF REGISTRAR ACCREDITATION AGREEMENT sent by the Internet Corporation for Assigned Names and Numbers (ICANN) to the CEO of the company (Figure 28).

Great! We have the CEO and company address. Unfortunately, this letter is from 2013 and searching various online databases and maps show no sign of GalComm or a related business at the address given in this letter.

Given they are an internet technology company, GalComm has shockingly little presence on the internet (Figure 29). This is similar to the scenarios encountered when trying to investigate malware domains. There is frequently little to find in internet searches for malicious domains (and registrars?), by design.

Is Something Seriously Broken in the Oversight Infrastructure for Domain Name Registrars ?

This report shows that one of the organizations that is key to the functioning of the internet, a registrar who maintains a Registrar Accreditation Agreement with ICANN, is responsible for far more malicious domains, malware, and exploitative content on the internet than legitimate content.

This begs the questions:

- When a registrar can wield this much power and introduce this much risk (and in some ways, instability) into the internet, who should be providing oversight of registrar activity?
- If oversight is supposed to exist, why does it fail in cases like this?
- Who should be accountable when a registrar engages in activity like this?

ICANN has a very small amount of verbiage in their Registrar Accreditation Agreement, as shown below: (emphasis added by the author.)

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). **Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.**

3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. **Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report.** In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 **Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports.** Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

And that's it.

Beyond this, the Registrar Accreditation Agreement completely disregards the lawfulness of the activity of the registrar.

In fact, even these minimal requirements from ICANN highlighted in the bolded text above are not being followed by GalComm. This lack of oversight by ICANN seems to point towards a general indifference to the implementation and execution of these rules. Perhaps more importantly, it contributes to the fact that the underlying internet infrastructure we rely and implicitly trust every day is more brittle than we've realized.

CIOs, CISOs and security teams in enterprises around the world are subject to extraordinary levels of audit, oversight, and accountability across countless regulations. How is it that the same does not apply to organizations like registrars, who, in many cases, can wield far more power to do harm?

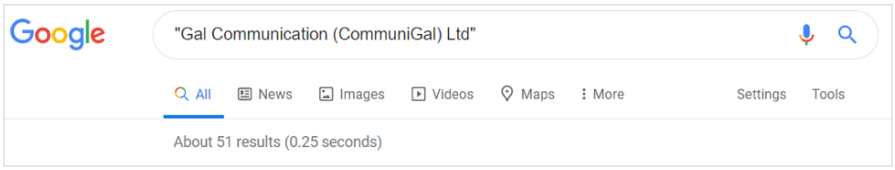


Figure 29: A total of 51 results (several of which are malware related) is a small number of results for a 20-year old internet registrar!

Their current address is given as:
24 Giborei Israel St.
Netanya, Israel

On the internet (including searching business databases in Israel), there is even less evidence of the company existing at this second address, although it is probably worth mentioning this second address is only a block away from the first (Figure 30).

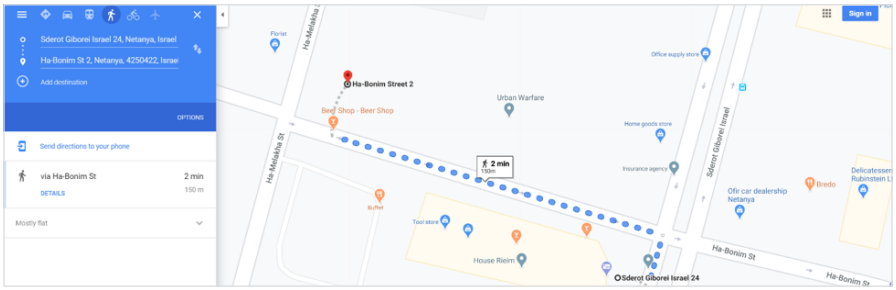


Figure 30: The two locations associated with GalComm over the past 10 years are very close to each other.

Pivoting off this second address, our investigation found the United States Food and Drug Administration's Office of Regulatory Affairs Health Fraud Branch (HFB) filed an abuse complaint[21] in 2019 against GalComm for a website **selling non-FDA approved abortion pills** Mifepristone and Misoprostol to US consumers (Figure 31). While this specific complaint is not believed to be tied to nefarious activities included in this report, datapoints like this help paint a picture about the type of registrants (end users) seeking GalComm.

There are several other types of formal and legal complaints found online about GalComm. The common thread they all share: there is no record of GalComm responding to any of the complaints. There is very little other information about the registrar, except a few reviews from people who seem to have stumbled into registering their domains with GalComm. Perhaps unsurprisingly, the reviews trend towards significantly negative (Figure 32).


U.S. FOOD & DRUG ADMINISTRATION

Abuse Complaint from the U.S. Food and Drug Administration - Office of Regulatory Affairs Health Fraud Branch (HFB)

REF: 264175

March 20, 2019

To:
Communigal Communication Ltd
www.galcomm.com
24 Giborei Israel st
Netanya Israel

Cc:
Verisign Worldwide Headquarters
www.verisign.com
12061 Bluemont Way
Reston, VA 20190
United States

Via email: support@galcomm.com and info@verisign-grs.com

The United States Food and Drug Administration is a consumer protection agency of the United States Government that is, among other things, responsible for regulating and supervising the safety of medical products and enforcing laws regulating medical products. Accordingly, we have determined that the website listed below is offering misbranded and unapproved new drugs, for sale to consumers in the United States in violation of the Federal Food, Drug and Cosmetic Act (FD&C Act) found at Title 21, United States Code, § 321, 331, 352, 353 and 355, et. seq.

The domain name below is registered by your company and is currently accessible to consumers in the United States:

Buyabortionpillrx.net

This website offers misbranded and unapproved new drugs (e.g. a combination pack of mifepristone and misoprostol tablets, marketed as "Abortion Pill Pack") for sale to U.S. consumers. These products appear to be new drugs as defined by section 201(p) of the FD&C Act, 21 U.S.C. §321(p), because they are "not generally recognized as safe and effective." Pursuant to section 505(a) of the Act, 21 U.S.C. §355(a), a new drug may not be introduced or delivered for introduction into interstate commerce unless it is the subject of an approved application. In addition, the introduction or delivery for introduction of such misbranded and unapproved new drug products into U.S. interstate commerce is a prohibited act per section 301 of the Act, 21 U.S.C. §321.

Furthermore, under U.S. law, prescription drugs can be dispensed only pursuant to a prescription from a healthcare practitioner licensed by law to administer prescription drugs. Offering new drugs without requiring a prescription jeopardizes patient safety and misbrands the drug under section 503(b)(1) of the FD&C Act. Dispensing a prescription drug without a prescription is an act which results in the drug being misbranded while held for sale, in violation of section 301(k) of the FD&C Act (21 U.S.C. § 331(k)).

This is an abuse complaint submitted to you under Section 3.18.2 of the 2013 ICANN Registrar Accreditation Agreement (RAA) regarding the use of domain names for illegal purposes. The 2013 RAA contains requirements pertaining to your duty to investigate and respond appropriately to reports of illegal activity (Sections 3.18 and 1.13). An appropriate response to this complaint would be to ensure that this website is not able to sell or otherwise offer for sale any unapproved drugs or undisclosed devices, or potentially counterfeit, controlled, adulterated or misbranded products to U.S. consumers in violation of U.S. law.

Figure 31: Abuse Complaint from the U.S. Food and Drug Administration - Office of Regulatory Affairs Health Fraud. https://www.fda.gov/consumers/communigal-communication-ltd-abortionpillrxnet

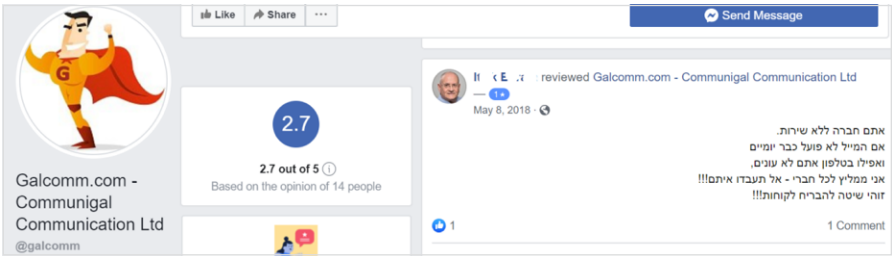


Figure 32: Most reviews are very negative. For those who don't speak Hebrew, Google Translate can provide some colorful insights.

21 https://www.fda.gov/consumers/communigal-communication-ltd-abortionpillrxnet

The InstallCore – GalComm Nexus

But wait, there's more! As Figure 33 shows, searching for the IOCs highlighted in Chapter 2 returns results that are only associated with GalComm-registered domains (shown in the red box).

Red box

All the results for these IOCs are GalComm-registered domains.

Blue box

Although this report contains approximately 15,000 domains used over the past couple of years, individual campaign activity tends to be executed within smaller windows of time. In Figure 33, this campaign has been most active within the past 30 days.

Orange box

Zero detections in VirusTotal across 80 different security products.

Purple box

403 (Forbidden) errors, which as described in Chapter 3, is subtly why all of these samples have zero detections.

The purple box is perhaps the most impactful finding as it relates to the security industry and is why Chapter 3 is dedicated to it. It is also a uniquely curious characteristic of most malicious domains registered by GalComm.

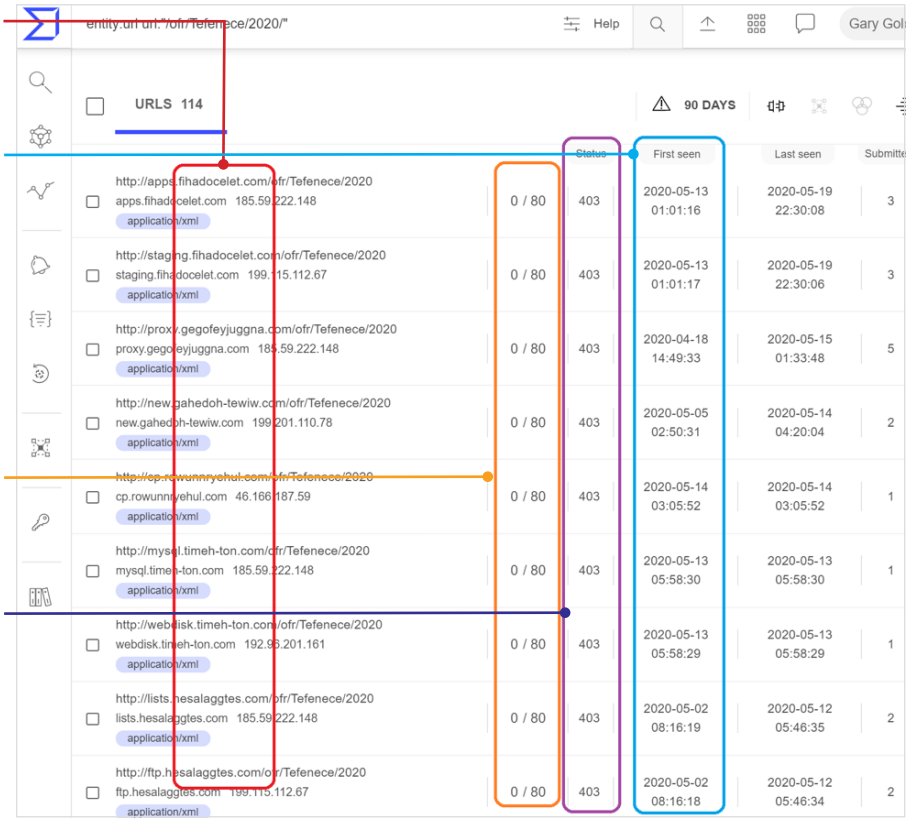


Figure 33: Searching for the same IOCs returns only GalComm-registered domains.

Is GalComm Malicious, or Are They Innocent and Being Taken Advantage Of?

This is one of the most important questions we looked to answer as part of our research. If we look at currently active domains registered through GalComm, they are responsible for putting more malicious domains and content on the internet than legitimate domains. If guilt is established by association, then yes, they are malicious.

Awake threat researchers also made several attempts to contact GalComm by phone, email (abuse@, security@, and support@), and the contact form on their website to notify them about the domains, associated malicious activity, and to get answers to the following questions.

Q:	**What is GalComm's policy on taking down (or blocking) domains being used exclusively for malicious purposes?**
Q:	**How are the people behind these domains able to acquire so many of them through GalComm?**
Q:	**Given these domains account for approximately 60% of the total domains GalComm currently has on the internet, how could this go unnoticed by the company?**

In fact, as we discuss in the sidebar, ICANN accreditation states that registrars need to publish contact information and policies for dealing with domains they have sold that are used for unlawful activity, in addition to setting standards for responding to complaints. We found none of this information published by GalComm.

After sending notifications via email, web form, and phone on April 29, 2020, then resending the notification again nine days later, we have received no response from GalComm at publishing time of this paper, nor have we observed any decrease in malicious activity associated with their domains. In fact, a very recent observation (in the days before the publishing of this paper, yet after notifications had been sent) appeared to show an increase in both volume and sophistication of malicious GalComm registered domain activity.

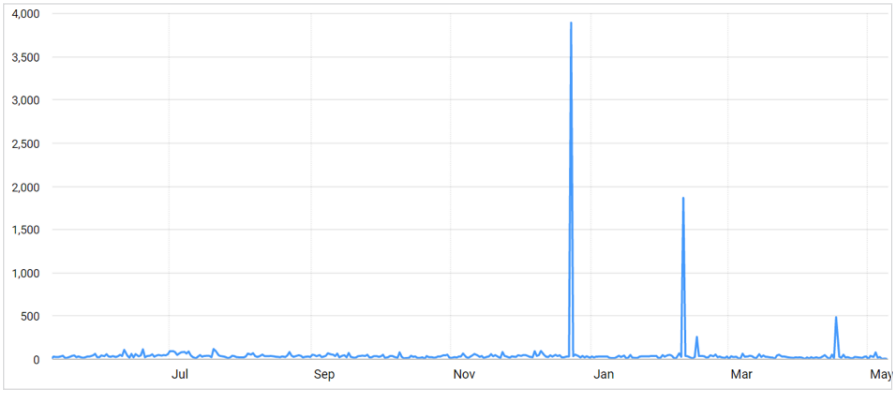


Figure 34: The count of daily registrations made by GalComm over the past year. A single day in December accounted for almost 20% of all their active domains on the internet at that time. Domains registered within these spikes have been used in malicious activity observed "in the wild." It's extremely difficult to imagine a scenario where such massive orders of domains go completely unnoticed and unquestioned by the GalComm team.

In summary, given the sheer volume of maliciousness put onto the internet by GalComm, and the lack of response or action to reduce the threats associated with the domains, we believe GalComm is, at best complicit in the threats described within this report.

Loose-Ends and Unanswered Questions about GalComm

There are a few outstanding questions remaining that have not been fully explored at the time of publication. We discuss these next to spur broader research across the community.

The Curious Case of rtb-seller[.]com

There is one GalComm domain that stands apart from the others, rtb-seller[.]com. This domain was observed in every organization analyzed. It does share a significant number of the TTPs of other known bad GalComm C2 domains but is far more prevalent than any other domains.

This domain appears in several advertising network blocklists. Its behavior on the network is indeed congruent with advertising network related activity. By that, we mean it is not persistent with a discernable pattern, if it even appears more than once for a given device. Additionally, it always co-occurs when the user is actively surfing the web, typically while reading high-reputation web pages filled with advertisements. However, rtb-seller.com activity in the wild is also quite different from all other advertising network traffic. For starters, we frequently see encrypted tunnels to rtb-seller.com where the client is **uploading encrypted data** to rtb-seller.com, **not downloading it.**

However, because the activity seems to be related to the incredibly complex world of ad selection, predictability triggering this activity for meaningful testing and research purposes has been difficult. One theory about rtb-seller.com is that it's used to op-

22 https://en.wikipedia.org/wiki/Real-time_bidding#Privacy_and_security
23 https://www.monetizemore.com/blog/real-time-bidding-rtb-explained/
24 https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf
25 https://www.icann.org/registrar-reports/accreditation-qualified-list.html

portunistically target very specific users/demographics via ad exchanges using real-time bidding[22] through 3rd party demand side platforms (DSPs). If you're not familiar with how ad selection works, yes, it is indeed incredibly complex![23]

A recent report[24] on real-time bidding published by the UK's regulator responsible for data protection, found these platforms have been "collecting and trading information such as race, sexuality, health status or political affiliation" without consent from affected users and "sharing people's data with potentially hundreds of companies, without properly assessing and addressing the risk of these counterparties..."

While research into this domain is ongoing, we recommend blocking rtb-seller[.]com within the organization. In the best-case scenario, it's only ads. **In the worst case, it could be an incredibly prolific intelligence collection or misinformation campaign.**

Are These Other Companies Also Engaged in Shady Practices?

In performing our research, we observed the Google advertising ID used by GalComm (UA-15374292) is also used by the following companies:

- BigNet Internet Solutions (bignet.co.il)
- Mobik (mobik.co.il, mobik.mobi, and mobikapp.com)
- webhostingservices.info

The connection between these companies and GalComm runs deeper than shared Google advertising IDs. It appears that these companies share the same principals as well. We also see other interesting connections. For instance, Mobik uses the same corporate phone number as GalComm and BigNet shares the same corporate address as GalComm. It is worth pointing out that GalComm is registered in Israel's government registry of companies, but neither Mobik nor BigNet are listed.

Although Mobik does not seem to be a registered company in Israel, it is notable that, like GalComm, Mobik is currently an ICANN accredited registrar. In fact, Israel has five ICANN accredited registrars[25], however three of those five, GalComm, Mobik and SiteName Ltd., appear to be connected to the same principals. While our research focused on GalComm, initial analysis of the other two indicates that they have their fair share of nefarious activity as well. As an example, a sampling of domains that appear to be created for typo-squat attacks targeting Google websites and registered through Mobik are provided in Appendix D.

Summary

Awake uncovered 15,160 domains tied to exploitive landing pages, malicious chrome extension command and control, and related malware. 111 fake and malicious chrome extensions associated with these attack campaigns were harvested in the wild from enterprise networks in only the past three months. These extensions were performing operations such as taking screenshots of the victim device, loading other malware, reading the clipboard, and actively harvesting tokens and user input. In fact, Google has taken down these extensions following Awake reporting these malicious behaviors to them. Awake discovered this activity in most of the enterprise networks investigated both in the US and abroad.

Awake also observed these campaigns engaged in a significant amount of evasive techniques to avoid being added to blocklists / labelled as malicious by cloud-based sandboxes, domain classification engines, reputation checkers, online virus scanners, etc. In fact, most of these popular security research tools label the domains as “safe” or “parked” at worst.

We also observed this campaign using custom Chromium packages to preinstall the malicious extensions while bypassing the Chrome Store’s security checks. Moreover, even the “fake” extensions in the Chrome Store appeared to have artificially inflated download counts and positive reviews, to trick users into downloading what they think is a popular extension. These fake extensions appear to do little more than collect information.

Finally, the one thread that connects all of this is GalComm, the registrar for the domains used for command and control, host for malicious Chrome extensions and the destination for exfiltrated data.

Lessons for Enterprise Security Teams

These are some of the key lessons for enterprise security teams based on the findings of this threat research:

- Rogue browser extensions are a higher risk threat than most people realize, especially as more of our digital life is now conducted within the browser.
- Domain classification engines, security proxies, online reputation checkers, cloud-based sandboxes, and most cloud-based security technologies can be substantially inaccurate because of simple defensive techniques employed by the adversary. Security teams should therefore be cautious in relying primarily on these kinds of tools.
- Similarly, EDR solutions frequently have difficulty identifying suspicious browser extensions.
- Applications detected as PUPs frequently have all the same characteristics of full-fledged malware.
- Combined full packet capture (FPC) forensics and network traffic analysis (NTA) solutions can effectively compensate for the security weaknesses highlighted in this report. Solutions like Awake are purpose-built to truly be your last line of defense. More specifically, the use of adversarial modeling makes it possible to automate the hunt for threat actor TTPs like those illustrated in this paper.

Appendix A

List of GalComm Registered Domains Used for C2 or Exploitation

List of domains associated with any malicious and / or suspicious activity analyzed as part of this report can be found here.

Appendix B

List of Malicious Chrome Extensions Discovered in Enterprise Networks Using GalComm Registered Domains for Command and Control (C2)

acmnokigkgihogfbeookIgemindnbine	ggijmaajgdkdijomfipnpdfijcnodpip	lnedcnepmplnjmfdiclhbfhneconamoj
apgohnlmnmkblgfplgnlmkjcpocgfomp	ghgjhnkjohlnmngbniijbkidigifekaa	lnlkgfpceclfhomgocnnenmadlhanghf
apjnadhmhgdobcdanndaphcpmnjbnfng	gllihgnfnbpdmnppfjdlkciijkddfohn	loigeafmbglngofpkkddgobapkkcaena
bahkljhhdeciiaodlkppoonappfnheoi	gmmohhcojdhgbjjahhpkfhbapgcfgfne	lpajppfbbiafpmbeompbinpigbemekcg
bannaglhmenocdjcmlkhkcciioaepfpj	gofhadkfcffpjdbonbladicjdbkpickk	majekhlfhmeeplofdolkddbecmgjgplm
bgffinjklipdhacmidehoncomokcmjmh	hapicipmkalhnklammmfdblkngahelln	mapafdeimlgplbahigmhneiibemhgcnc
bifdhahddjbdbjmiekcnmeiffabcfjgh	hijipblimhboccjcnnjnjelcdmceeafa	mcfeaailfhmpdphgnheboncfiikfkenn
bjpknhldlbknoidifkjnnkpginjgkgnm	hmamdkecijcegebmhndhcihjjkndbjgk	mgkjakldpclhkfadefnoncnjkiaffpkp
blngdeeenccpfjbkolalandfmiinhkak	hodfejbmfdhcgolcglcojkpfdjjdepji	mhinpnedhapjlbgnhcifjdkklbeefbpa
ccdfhjebekpopcelcfkpgagbehppkadi	hpfijbjnmddglpmogpaeofdbehkpball	mihiainclhehjnkljjgpokdpldjmjdap
cceejgojinihpakmciijfdgafhpchigo	ianfonfnhjeidghdegbkbbjgliiciiic	mmkakbkmcnchdopphcbphjioggaanmim
cebjhmljaodmgmcaecenghhikkjdfabo	ibfjiddieiljjjccjemgnoopkpmpniej	mopkkgobjofbkkgemcidkndbglkcfhjj
chbpnonhcgdbcpicacolalkgjlcjkbbd	inhdgbalcopmbpjfincjponejamhaeop	mpifmhgignilkmeckejgamolchmgfdom
cifafogcmckphmnbeipgkpfbjphmajbc	iondldgmpaoekbgabgconiajpbkebkin	nabmpeienmkmicpjckkgihobgleppbkc
clopbiaijcfolfmjebjinippgmdkkppj	ipagcbjbgailmjeaojmpiddflpbgjngl	nahhmpbckpgdidfnmfkfgiflpjjilce
cpgoblgcfemdmaolmfhpoifikehgbjbf	jagbooldjnemiedoagckjomjegkopfno	ncepfbpjhkahgdemgmjmcgbgnfdinnhk
dcmjopnlojhkngkmagminjbiahokmfig	jdheollkkpfglhohnpgkonecdealeebn	npaklgbiblcbpokaiddpmmbknncnbljb
deiiiklocnibjflinkfmefpofgcfhdga	jfefcmidfkpncdkjkkghhmjkafanhiam	npdfkclmbnoklkdebjfodpendkepbjek
dipecofobdcjnpffbkmfkdbfmjfjfgmn	jfgkpeobcmjlocjpfgocelimhppdmigj	nplenkhhmalidgamfdejkblbaihndkcm
dopkmmcoegcjggfanajnindneiffffpck	jghiljaagglmcdeopnjkfhcikjnddhhc	oalfdomffplbcimjikgaklfamodahpmi
dopmojabcdlfbnppmjeaajclohofnbol	jgjakaebbliafihodjhpkpankimhckdf	odnakbaioopckimfnkllgijmkikhfhhf
edcepmkpdojmciieeijebkodahjfliif	jiiinmeiedloeiabcgkdcbbpfelmbaff	oklejhdbgggnfaggiidiaokelehcfjdp
ekbecnhekcpbfgdchfjcfmnocdfpcanj	jkdngiblfdmfjhiahibnnhcjncehcgab	omgeapkgiddakeoklcapboapbamdgmhp
elflophcopcglipligoibfejllmndhmp	jkofpdjclecgjcfomkaajhhmmhnninia	oonbcpdabjcggcklopgbdagbfnkhbgbe
eogfeijdemimhpfhlpjoifeckijeejkc	kbdbmddhlgckaggdapibpihadohhelao	opahibnipmkjincplepgjiinbfmppmh
fcoboklibIbalmjmahdebcdalglnieii	keceijnpfmmlnebgnkhojinbkopolaom	pamchlfnkebmjbfbknoclehcpfclbhpl
fgafnjobnempajahhgebbbpkpegcdlbf	khhemdcdllgomlbleegjdpbeflgbomcj	pcfapghfanllmbdfiipeiihpkojekckk
fgcomdacecoimaejookmlcfogngmfmli	kjdcopljcgiekkmjhinmcpioncofoclg	pchfjdkempbhcjdifpfphmgdmnmadgce
fgmeppijnhhafacemgoocgelcflipnfd	kjgaljeofmfgjfipajjeeflbknekghma	pdpcpceofkopegffcdnffeenbfdldock
fhanjgcjamaagccdkanegeefdpdkeban	labpefoeghdmpbfijhnnejdmnjccgplc	pgahbiaijngfmbbijfgmchcnkipajgha
flfkimeelfnpapcgmobfgfifhackkend	lameokaalbmnhgapanlloeichlbjloak	pidohlmjfgjbafgfleommlolmbjdcpal
fmahbaepkpdimfcjpopjklankbbhdobk	lbeekfefglldjjenkaekhnogoplpmfin	pilplloabdedfmialnfchjomjmpjcoej
foebfmkeamadbhjcdglihfijdaohomlm	lbhddhdfbcdcfbbbmimncbakkjobaedh	pklmnoldkkoholegljdkibjjhmegpjep
fpngnlpmkfkhodklbljnncdcmkiopide	ldoiiiffclpggehajofeffljablcodif	pknkncdfjlncijifekldbjmeaiakdbof
gdifegeihkihjbkkgdijkcpkjekoicbl	lhjdepbplpkgmghgiphdjpnagpmhijbg	plmgefkiicjfchonlmnbabfebpnpckkk
gfcmbgjehfhemioddkpcipehdfnjmief	ljddilebjpmmomoppeemckhpilhmoaok	pnciakodcdnehobpfcjcnnlcpmjlpkac
gfdefkjpjdbiiclhimebabkmclmiiegk	ljnfpiodfojmjfbiechgkbkhikfbknjc	ponodoigcmkgldd|ljanchegmkgkhmgb

Appendix C

Small Clusters of Similar TTP Domains; Clusters Related to Domain Distributing Custom Chromium Package

1: Completely Matching TTP Cluster

bbtwf[.]com	fahugugo[.]com	pawasor[.]com
bmjhc[.]com	hadopaf[.]com	qgmns[.]com
bwnbr[.]com	hdrbr[.]com	qofod[.]com
dbdrq[.]com	kabafahu[.]com	qofom[.]com
dfcsp[.]com	mbnrn[.]com	wcysr[.]com
dregsr[.]com	mopuf[.]com	wncysr[.]com

2: Closely Matching TTP Cluster

exposure4u.co.il
mystts[.]com
turbo-pixel[.]com
yoavofek.co.il
ypixl[.]com
alliancedownload[.]com
anchordownload[.]com
arcticdownload[.]com
ariebellzzxvqtesterrr[.]com
ariezzxvqtesterrr[.]com
auroradownload[.]com
automobiledownload[.]com
bestfreefilesfordownload[.]com
bestfreewebgames[.]com
bestwindowsretrogames[.]com
blitzdownload[.]com
blueskydownload[.]com
branchdownload[.]com
buyonlyoldusedgames[.]com
cadtoolforwin10[.]com
canvasdownload[.]com
cardownload[.]com
charterdownload[.]com
checkyourgameschartpos[.]com
downloadalpha[.]com
downloadanalyst[.]com
downloadbeyond[.]com
downloadbrite[.]com
downloadcharter[.]com
downloadchick[.]com
downloadcollections[.]com
downloadcollector[.]com
downloadcove[.]com
downloaddish[.]com
downloaddraw[.]com
downloadgeneral[.]com
downloadhotline[.]com
downloadlance[.]com
downloadnumber[.]com
downloadorama[.]com
downloadpunch[.]com
downloadscapes[.]com
downloadselection[.]com
downloadshape[.]com
downloadsyndicate[.]com
downloadtales[.]com
downloadunity[.]com
downloadvest[.]com
empowerdownload[.]com
eternaldownload[.]com
falcondownload[.]com
fixmyoldgames[.]com
fleamarketusedgames[.]com
formarketusedoldgames[.]com
freebuildgames[.]com
freec64games[.]com
freecolecogames[.]com
freefunctionorg[.]com
freemycats[.]com
freemyretrogames[.]com
freenewpeoplehere[.]com
freenewwebgames[.]com
freepdfmergetool[.]com
freewebgamesfordownload[.]com
freewindowsretrogames[.]com
freeyourbestwebgames[.]com
genesisdownload[.]com
geniedownload[.]com
groovydownload[.]com
harvestdownload[.]com
horseshoedownload[.]com
hrearethebestfilesfordownload[.]com
identitydownload[.]com
jointdownload[.]com
jointforfilesdownload[.]com
jointmyfilesdownload[.]com
juicytomatoesdownload[.]com
kentfrycans[.]com
labdownload[.]com
leaddownload[.]com
leatherdownload[.]com
lightningboltdownload[.]com
livingdownload[.]com
lookforthebestfile[.]com
lookforthebestfileintheworld[.]com
lunardownload[.]com
medidownload[.]com
motorcardownload[.]com
mybestfilesfordownload[.]com
mybestplaceforfilestodownload[.]com
myfreeretrogames[.]com
newwavethebestintheworld[.]com
nitrogendownload[.]com
northfielddownload[.]com
olivedownload[.]com
ordinarylabratorydownload[.]com
outletdownload[.]com
panrtodelare[.]com
placefordownload[.]com
placeforfilestodownload[.]com
popmusicisthebestmusic[.]com
powderdownload[.]com
primodownload[.]com
productiondownload[.]com
rallydownload[.]com
rdnld[.]com
rhinodownload[.]com
rhtab[.]com
routedownload[.]com
ruraldownload[.]com
safenewforbusypeople[.]com
sec4biz.co.il
shoredownload[.]com
smokeboundarydownload[.]com
snowplowdownload[.]com
sonatadownload[.]com
strongtreedownload[.]com
synthpopthebestmusicintheworld[.]com
tacticaldownload[.]com
takejointforfilesdownload[.]com
thebestplaceforfilestodownload[.]com
trafficdownload[.]com
trenddownload[.]com
tropicaldownload[.]com
universedownload[.]com
venuedownload[.]com
warriordownload[.]com
whatisthebestplaceforfilesfordownload[.]com
whatwindowsretrogames[.]com
whereareymybestfilesfordownload[.]com
wherearethebestfile[.]com
wherearethebestplaceforfilestodownload[.]com
wildernessdownload[.]com
yourbestplaceforfilestodownload[.]com

Appendix D

Sample of Suspicious Mobik Registered Domains

The list below contains a small sample of domains that appear to be designed for typo-squat attacks targeting Google. These domains have been registered through the registrar MOBIKAPP and is discussed in Chapter 3.

abcyoutube[.]com	googlemqil[.]com	segoogle[.]com
bajarmusicayoutube[.]com	googlenewssubmit[.]com	segredosgooglenews[.]com
convertidordeyoutubemp3[.]net	google-obrazky[.]com	signintogmail[.]com
crearcuentagoogle[.]com	googlepixelmanuals[.]net	ss-youtube[.]com
dwnyoutube[.]com	googleplas[.]com	storegoogle[.]com
fastestyoutubedownloader[.]com	googleplaystor[.]com	tubemateyoutubedownloader[.]com
firebasegoogle[.]com	googleplaystoreapks[.]com	vidyoutube[.]com
fogoogle[.]com	googleplsy[.]com	workingforgoogle[.]com
frgmail[.]com	googleprank[.]com	wweyoutube[.]com
frgoogle[.]com	googlerive[.]com	xn--gmail-rta[.]com
gigoogle[.]com	googlesettings[.]com	xn--googlebersetzer-4vb[.]com
gmailaa[.]com	googletagservice[.]com	xn--ssyoutube-r3a[.]com
gmaille[.]com	googletrad[.]com	xn--wwwgoogle-d4a[.]com
gmailol[.]com	googletranclate[.]com	yiyoutube[.]com
gmailpassrecovery[.]com	googlevdeo[.]com	yogoogle[.]com
gmail-signup[.]com	googlevedio[.]com	youtube2dvd[.]com
google444[.]com	googleweblight[.]net	youtubebuddy[.]com
googleaearth[.]com	googlyoutube[.]com	youtubeco[.]com
googleblack[.]com	hackyoutube[.]com	youtubecreators[.]com
googlebussines[.]com	listetoyoutube[.]com	youtubeeee[.]com
googlecalender[.]com	miyoutube[.]com	youtubefreemovie[.]com
googlecharme[.]com	mygmailsignin[.]com	youtubegmail[.]com
googlechromo[.]com	neewgoogle[.]com	youtubehack[.]com
googlecrohme[.]com	newgmailaccount[.]com	youtubehoo[.]com
googledrie[.]com	newyoutube[.]com	youtube-movies[.]net
googleespn[.]com	ns1google[.]com	youtubemp3donusturucu[.]net
googlefamilyfeud[.]com	ooggoogle[.]com	youtuberipper[.]com
googleindir[.]com	ooyoutube[.]com	youtubetu[.]com
googlemaail[.]com	orgoogle[.]com	youtubeunblocked[.]net
googlemaprs[.]com	ritgmail[.]com	youtubexx[.]com
googlemapsd[.]com	santatrackergoogle[.]com	youtubeyo[.]com
googlemasil[.]com	schoolyoutube[.]com	ytyoutube[.]com
googlemerchant[.]com		

For additional information about Awake please visit awakesecurity.com

About Awake Security

Awake Security is the only advanced network traffic analysis company that delivers answers, not alerts. By combining artificial intelligence with human expertise, Awake models and hunts for both insider and external attacker behaviors, while providing full forensics across traditional, IoT and cloud networks for autonomous triage and response. The platform is ranked #1 by EMA for time to value and was recognized as the #1 information security solution being evaluated by global 1000 companies in Enterprise Technology Research's (ETR) Summer 2019 Emerging Technology Study.