Illicit Brand Impersonation | A Threat Hunting Approach

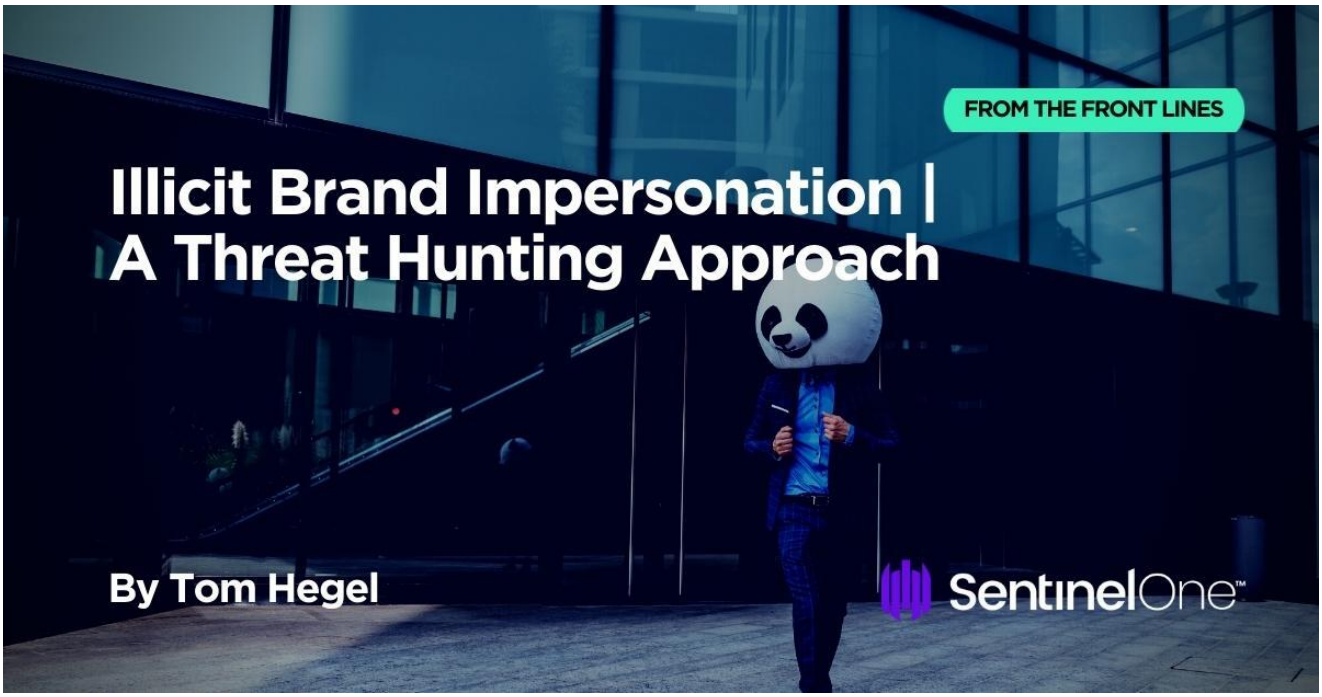
sentinelone.com/blog/illicit-brand-impersonation-a-threat-hunting-approach/

August 1, 2023

Since the start of 2023, brand impersonation has become the center of many questions we receive from everyday network defenders. While at the start of the year we reported on the heavy spike in malicious Google search ads, the activity continues to this day across many platforms, and does not get as much attention as it deserves. Additionally, while tracking more capable and often state-sponsored threat actors, we continually observe brands being impersonated for illicit use, including credential phishing and malware delivery.

Consequently, organizations find themselves grappling with two critical challenges: first, identifying and thwarting illicit brand impersonation aimed at targeting them, and second, effectively safeguarding their networks and users. Security and threat researchers face a similar, albeit magnified, responsibility as they handle these concerns for numerous entities.

Let's explore some examples of opportunistic and targeted threat actors impersonating trusted brands and how security researchers can make use of new tooling for the purposes of hunting and tracking them moving forward.



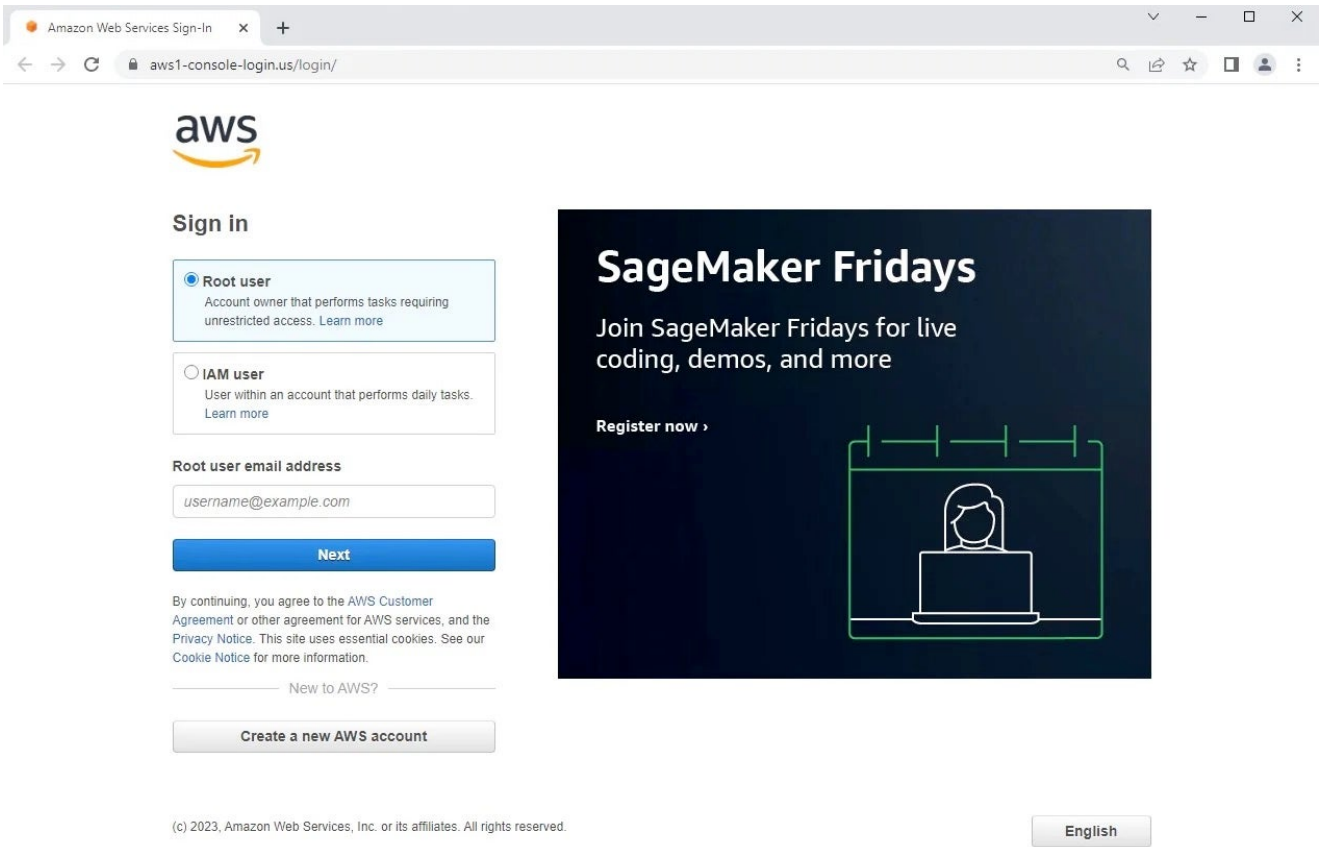
New Tools and Monitoring Techniques

VirusTotal has released a new feature called Netloc, essentially expanding the well known YARA engine to network telemetry and data. VirusTotal is a core resource for researchers, security vendors, network defenders, and even investigative journalists. With the incorporation of this new capability, it becomes imperative for others to familiarize themselves with and harness its full potential. Moreover, it exemplifies an approach that other security tools can and, indeed, should emulate in the context of engineering solutions for network data detection opportunities.

Many opportunities for hunting my favorite threat actors come to mind with this new capability. While APTs consume most of my attention, they are not the most common threat or concern for the majority of network defenders. For that, let's look at some malicious activity impacting far more organizations.

Mimicking Trusted Pages

In February of this year, we wrote about a campaign targeting cloud service credentials, specifically AWS logins. While the delivery of this is quite rare for the moment, being a direct Google advertisement, attackers continue to innovate through many other ways including phishing emails and non-Google ads to name only two.



Fake AWS Login Page

So how can we detect illicit login pages such as these? First, we have to note that many phishing pages reuse the content from the services they mimic, such as URL icons, body content, and images. If the VirusTotal scanner catches it fast enough, we can track down some commodity activity with this in mind.

```
import "vt"
rule aws_monitor {
        condition:
        vt.net.domain.new_domain and
        (vt.net.url.favicon.dhash == "4026d4f494f8738c" //AWS Name Icon
        or
        vt.net.url.favicon.dhash == "c8e3b88aaa88cbf8" //AWS Docs Icon
        or
        for any link in vt.net.url.outgoing_links: ( link matches
/signin.aws.amazon\.com.*/ )
        or
        vt.net.domain.raw matches /aws/)
}
```

This rule will trigger on any new URL which contains the same favicon used on the AWS login page or docs page, or contains an outgoing link to the legitimate AWS sign in page.

The main fear here is the potential for false positives or negatives, but that can be tuned with additional conditions of `vt.net.domain.new_domain` to weed out common legitimate domain hits, using VT tags, or simply reducing the condition specifics.

In many cases we've observed, a reuse of the favicon combined with a new domain can be quite wide and catch lots of interesting activity.

```
import "vt"
rule aws_monitor_2 {
    condition:
        vt.net.domain.new_domain and
        (vt.net.url.favicon.dhash == "4026d4f494f8738c" //AWS Name Icon
        or
        vt.net.url.favicon.dhash == "c8e3b88aaa88cbf8" //AWS Docs Icon
        )
}
```

AWS is just one example, threat hunters could instead use this for less common pages of value like download sites or internal intranet employee logins.

Reused Characteristics of Infrastructure – Commodity Targeting

One useful way to identify automated and often large-scale phishing campaign infrastructure is through monitoring and alerting on actor specific characteristics of their phishing sites.

Earlier this month Malwarebytes reported on malicious Google ads mimicking USPS with very realistic links, ultimately seeking mass collection of financial details. Looking into one of these domains (`super-trackings[.]com`), notice the reuse of a Yandex Tracker ID used for normal website analytics; however, this ID is owned by the specific threat actor associated with the USPS phishing campaign. The specific tracker is reused across the common `tracking.php` files, not the domain landing page.

Yandex Tracker 93030690

We can look back historically by searching for the tracker directly in VirusTotal. With many URL results, we can extract the following unreported phishing domains tied to the same actor:

```
uspps-onlynee[.]biz
hetclick[.]biz
uspps-only[.]ink
www.uspps-only[.]ink
super-trackings[.]com
uspps-onlyne[.]ink
usps.tracking-check[.]me
tracking-checks[.]me
goodstracks[.]me
usps-onlines[.]biz
diy-trackng[.]com
```

Instead of querying VirusTotal manually for this tracker within new URLs, let's instead monitor proactively to get alerts as soon as they are seen. For that, we can make use of a very simple rule monitoring for that same tracker.

```
import "vt"
rule usps_phisher_tracker {
    condition:
        for any tracker in vt.net.url.trackers: (
          tracker.id == "93030690")
}
```

A tracker can easily be changed by an actor, but the above example was used by the attacker from April to July 2023, so clearly they are rolled into new campaigns more than we might expect, depending on the attacker and campaign of course.

Reused Characteristics of Infrastructure – APTs

Even our more interesting APTs can be tracked in similar reuse of characteristics across their campaigns. Let's take a look at Kimsuky, one of a number of North Korean attributed threat actors we actively monitor.

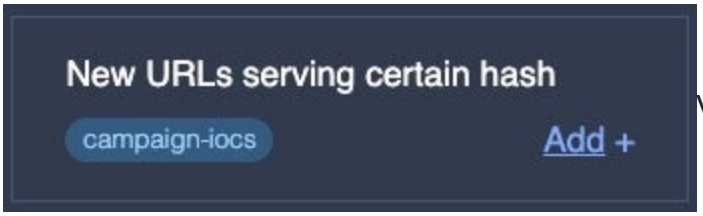
In May of this year, we wrote about Kimsuky evolving reconnaissance capabilities in a new global campaign, which was an interesting campaign making use of a new malware component we call ReconShark. In some of the malicious URLs, we can see the actor making use of a `config.php` file, reusing a small script for warning to enable JavaScript and acting as an input for credential theft functionality.

```
<!doctype html>
        <html>
        <head>
        <meta charset='utf-8'>
        <meta name='robots' content='noindex, nofollow, noarchive'>
        <meta name='viewport' content='width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no, user-scalable=0'>
        </head>
        <body style='background:#f8f8f8;color:#000000;padding:0;margin:0;'><br><p><center><noscript>You need to enable javascript</
        noscript></center></p>
        <script type='text/javascript'>
        var d = document;
        d.write("<br><br><form method='post'><center><input type='password' id='pass' name='pass'
            style='font-size:34px;width:34%;outline:none;text-align:center;background:#ffffff;padding:8px;border:1px solid
            #cccccc;border-radius:8px;color:#000000;'></center></form>");
        d.getElementById('pass').focus();
        d.getElementById('pass').setAttribute('autocomplete', 'off');
        </script>
        </body></html>

```

Kimsuky's *config.php*

The new VT templates save us time here, as we can hit a single button to get the rule nearly written for us:



VirusTotal Netloc Template

Passing in our `config.php` SHA256 hash, and renaming, we get the following rule:

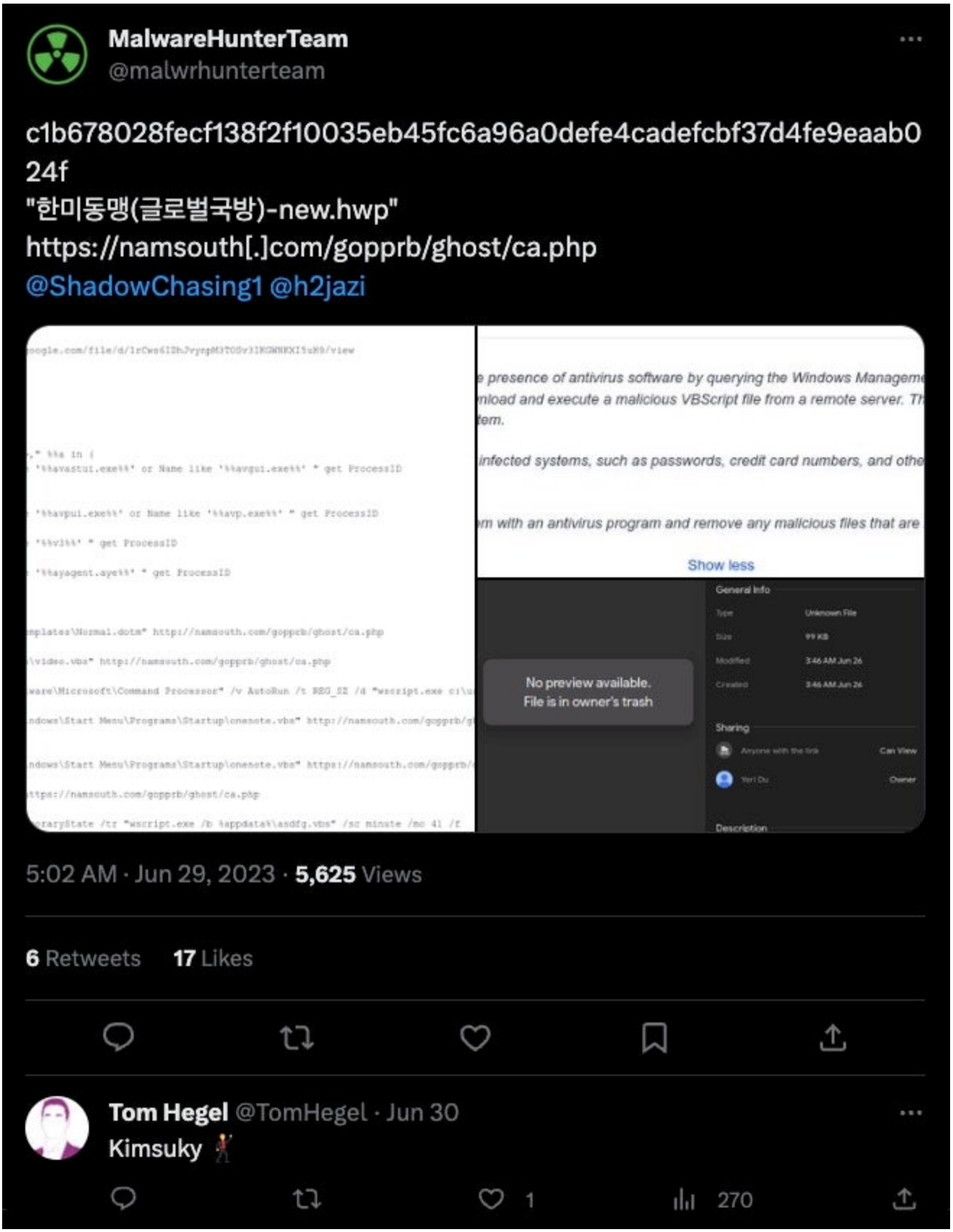
```
rule apt_nk_kimsuky_phishing_script {

    condition:
        vt.net.url.new_url and
        vt.net.url.downloaded_file.sha256 ==
"256fa5009e8e82258876325b7d36f41cc3e74e85627663206b042eec8736ce6a"

}
```

While beta testing Netloc with this rule, the file triggered across many unreported Kimsuky controlled URLs, and can also be found going back multiple years. In fact, while testing live detections, MalwareHunterTeam also happened to catch one, highlighting the pivot potential

to malicious Kimsuky attributed `.hwp` documents. This domain was later reported on by the AhnLab team. So not only does the technique work, it can lead to the discovery of interesting new APT brand-impersonating campaigns.



MalwareHunterTeam Kimsuky Linked Tweet

Here is a list of Domains/URLs which contain our Kimsuky `.php` file. Be warned, some of these are legitimate but compromised domains and go back a few years:

```
namsouth[.]com
nknews[.]pro/config.php
reasope[.]org/config.php
voesami[.]com/config.php
bit-albania[.]com/config.php
yonsei[.]lol/sss.php
jacobsenfamilyholdings[.]com/config.php
okbus.or[.]kr/config/config.php
renaissancenft[.]io/wp-content/plugins/download-plugin/plugins.php
stmwa[.]de/work/config/data.php
csmss[.]org/admin/uploads/award/award28.php
167.172.113[.]157/
108.179.214[.]134/
174.138.30[.]233/
absolutemedia[.]net.au/
absolutemedia[.]net.au/testing/wp-content/intelmanagertools.exe
absolutemedia[.]net.au/testing/wp-includes/Spectrum
absolutemedia[.]net.au/testing/flash-x32-adobe-add-on.exedl.netprog.net
absolutemedia[.]net.au/testing/flash-x32-Adobe-add-on.exe
eskulap-jarocin[.]pl/
blogtify[.]com/wp-includes/config.php
kevinspie.co[.]kr/data/category/faq/faq.php
hankevin.cafe24[.]com/data/category/faq/faq.php
educacionit[.]com/images-clientes/4O4.php
naturamosana[.]be/css/main.php
wincenty-faber[.]pl/ksiki/ksiki-dla-dzieci
wincenty-faber[.]pl/dla-dzieci
escolarainhadleonor[.]eu/aee/
wincenty-faber[.]pl/dla-dzieci/publikowane-w-ksikach/90
217.219.131[.]139/db.php
chromatogramma[.]ru/book/export/html/3
aprendizajevirtual.une[.]net.co/lang/language.php
```

This approach, again, may need fine-tuning depending on context, but it offers a good example of one way to do such tracking. There are many other methods available for successfully tracking Kimsuky brand impersonation and other actors including hostname similarities against their normally targeted organizations, or even URL patterns of known toolkits to name a few. Happy Hunting!

Conclusion

The persistent use of brand impersonation by opportunistic and sophisticated threat actors for illicit activities like credential phishing and malware distribution warrants greater awareness and technical capabilities.

By leveraging the latest tooling and staying vigilant, security and threat researchers can play a pivotal role in mitigating these risks for numerous organizations. As we continue to confront these challenges, it is essential to foster collaboration, knowledge sharing, and innovative solutions to stay ahead in the ever-evolving threat landscape.