

SharpPine

Pwning your foreign policy,
one interview request at a time

Tom Lancaster | VirusBulletin

5 October 2023

About Volexity

- Background

- ❑ Washington DC area-based security firm with global presence
- ❑ Founded: August 2013
- ❑ Core team: 11+ years
- ❑ Wrote the leading books on malware analysis and memory forensics

- Business Areas

- ❑ Information Security Services
 - Managed security, consulting, and threat intelligence
- ❑ Next-Generation Forensics/Security Products
 - Developed and maintained internally
 - Memory Acquisition (Surge) and Analysis (Volcano)
- ❑ Global Incident Response/Forensics Training
 - Public and private trainings

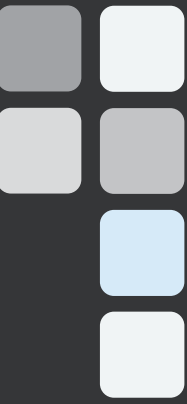
Customers

- Financial Services
- Technology Companies
- Defense Industrial Base
- Service Providers
- Energy
- Insurance
- NGOs & NPOs
- International Development
- Government Agencies

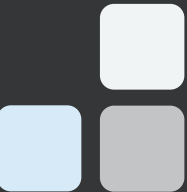
Agenda

- Who is SharpPine?
- Social Engineering & Phishing
- Infrastructure
- Malware
- Outlook





Who is SharpPine?



SharpPine? SharpTongue?

- It's just a name.
- Volexity moved to a new threat actor naming schema in Summer 2023.
- SharpPine == SharpTongue* (in the corresponding paper, and in the programme)



SharpPine Overview

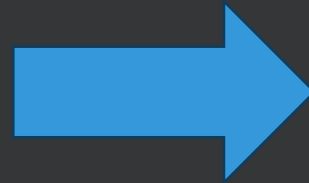
Attribute	Value
Country of Origin	North Korea 
Active Since	2012
Malware (current)	BabyShark, QuasarRAT, SHARPEXT, MISSDAISY, AMADEY & more.
Aliases	Kimsuky, APT43, Archipelago



What Does Success Look Like?

Attacker Goals

- Access to a user's mailbox.
- Facilitated through:
 - Credential theft
 - Use of malware
 - Keylogging
 - SHARPEXT (in-browser theft of mail)



Outcomes

- Insights into US/EU/KR foreign policy
 - redlines
 - “unofficial” positions
 - negotiation advantage
 - ... [other stuff]
- Better phishing against others




Previous Reporting

THREAT ANALYSIS GROUP

How we're protecting users from
government
North Korea

Apr 05, 2023
7 min read

New Threat A
stop governm

 Adam Weidemann
Threat Analysis Group

New BabyShark Security Think

John Hammond | 03.1.2022 | 31 Min Read

Targeted APT Activity: BABYSHARK Is Out for Blood

VOLEXITY // INTELLIGENCE

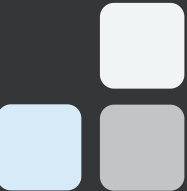
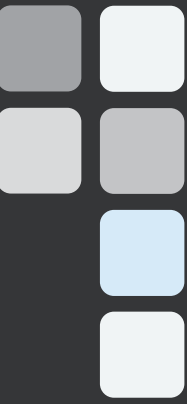
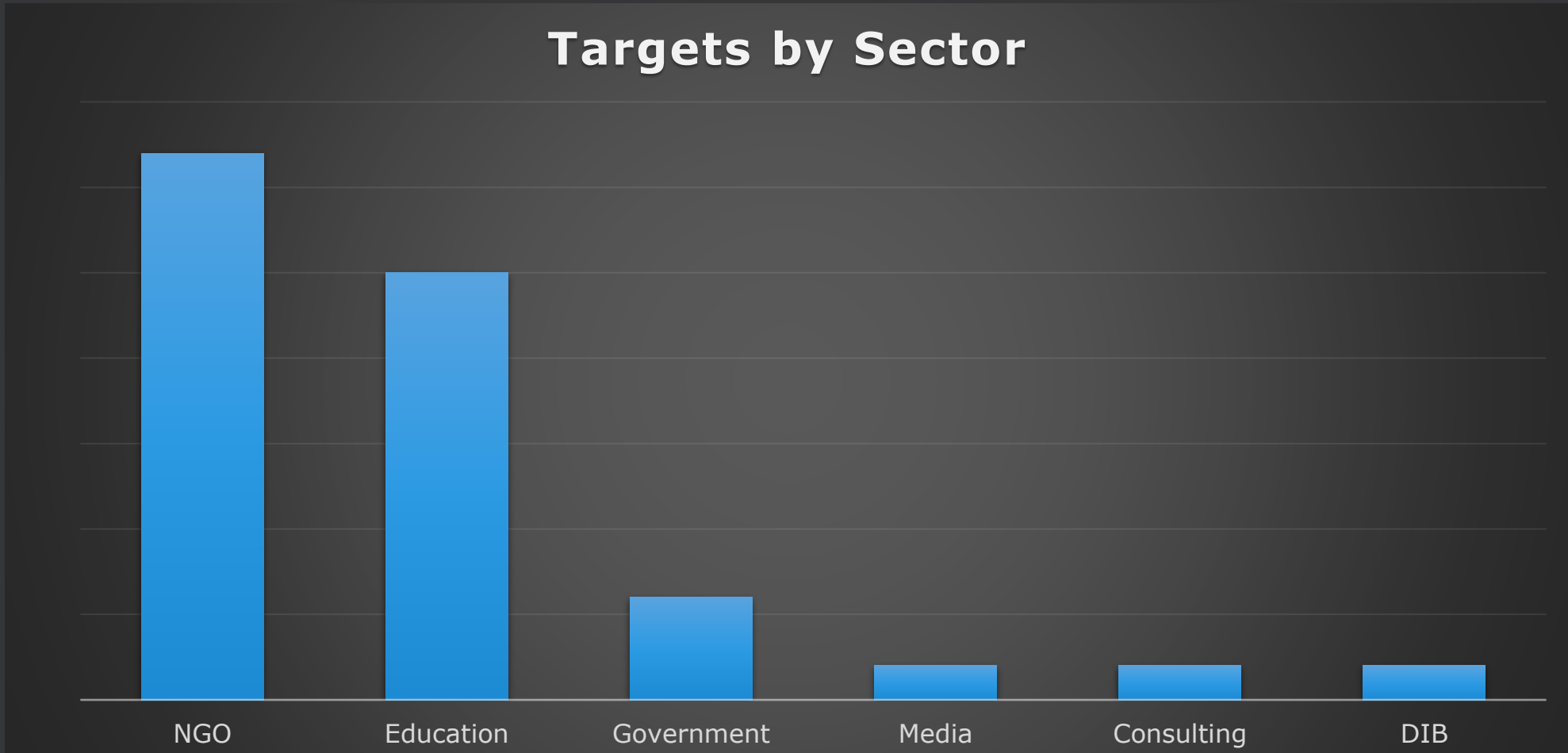
SharpTongue Deploys Clever Mail-Stealing Browser Extension "SHARPEXT"

- SharpTongue is a North Korean actor using newly discovered mail-theft malware, SHARPEXT
- Browser extension SHARPEXT steals mail data directly from webmail sessions
- Targeted users in USA, Europe, South Korea

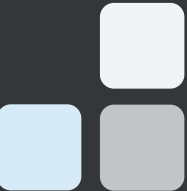
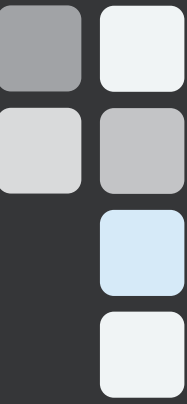
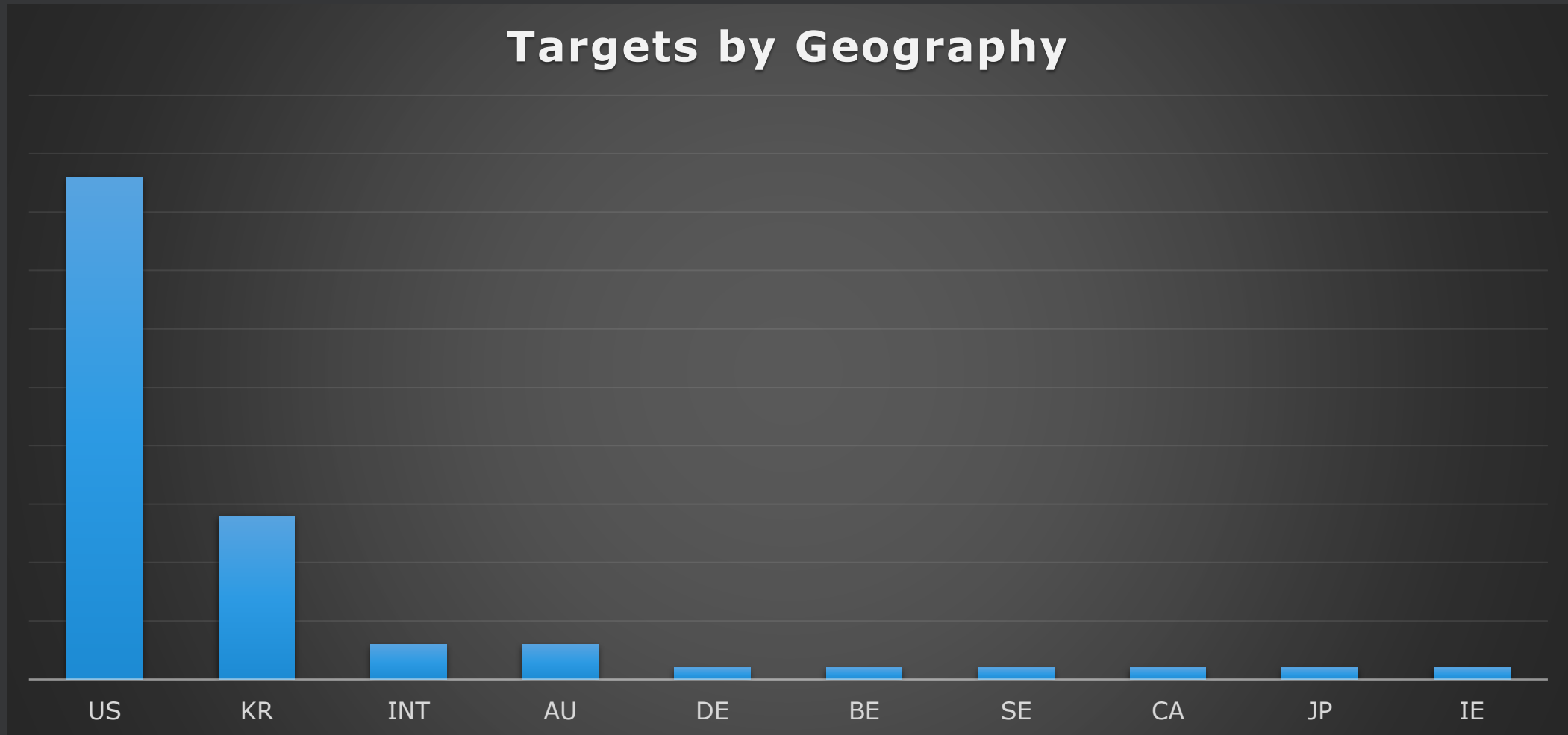


Group Uses
Espionage Operations

Targeting (Sector)



Targeting (Geography)

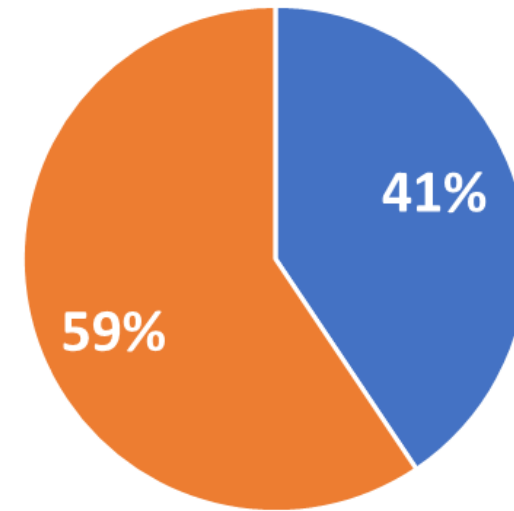


Targeting: This Time It's Personal

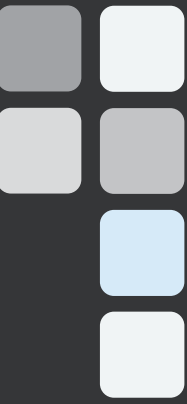
SharpPine is happy to compromise personal webmail accounts & devices.

- Targets often use personal mail for work purposes
- Webmail usually has no dedicated monitoring to identify phishing or compromise

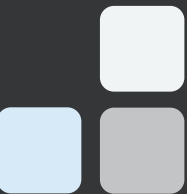
Distribution of Personal vs Organization Email in Typical SharpPine Phishing Campaign



■ Organization Email ■ Personal Email



Social Engineering & Phishing



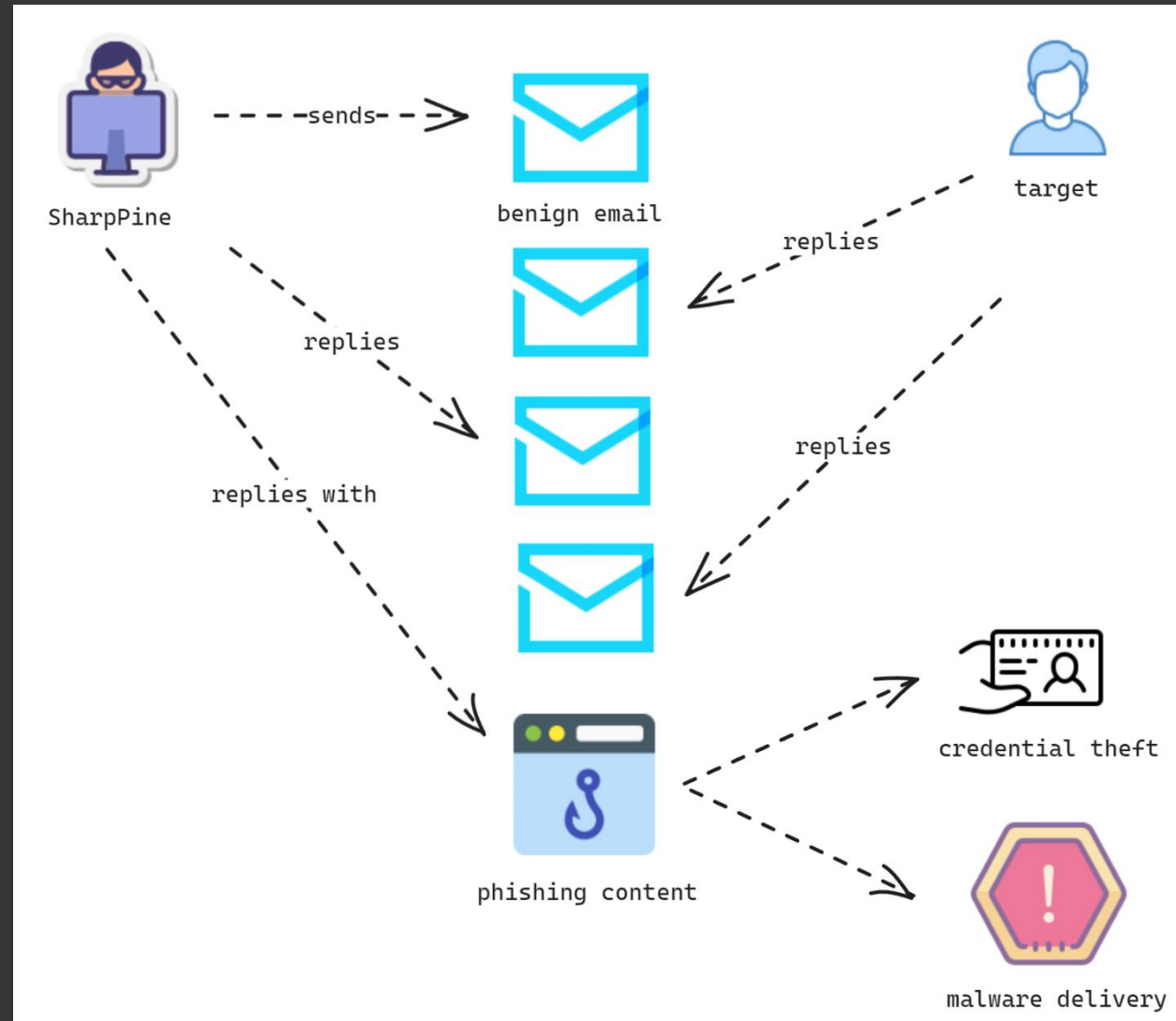
Master Social Engineers

- Rely on **subverting typical user workflows**
 - Targets regularly deal with mail from new senders sent via webmail.
 - Everyday work involves document review.
- Know Your ~~Customer~~ Phishing Targets
 - Email bodies powered by years of stolen mailbox data
 - Repurpose stolen content for decoy documents
 - Understanding of which experts know each other, how they talk to one another; what typical conversations they have
- Willing to build a conversation



Building a Conversation

- Helps defeat email detection methods
- Only send malware to people who are “expecting” the content.
- Ensures limited distribution of malware content

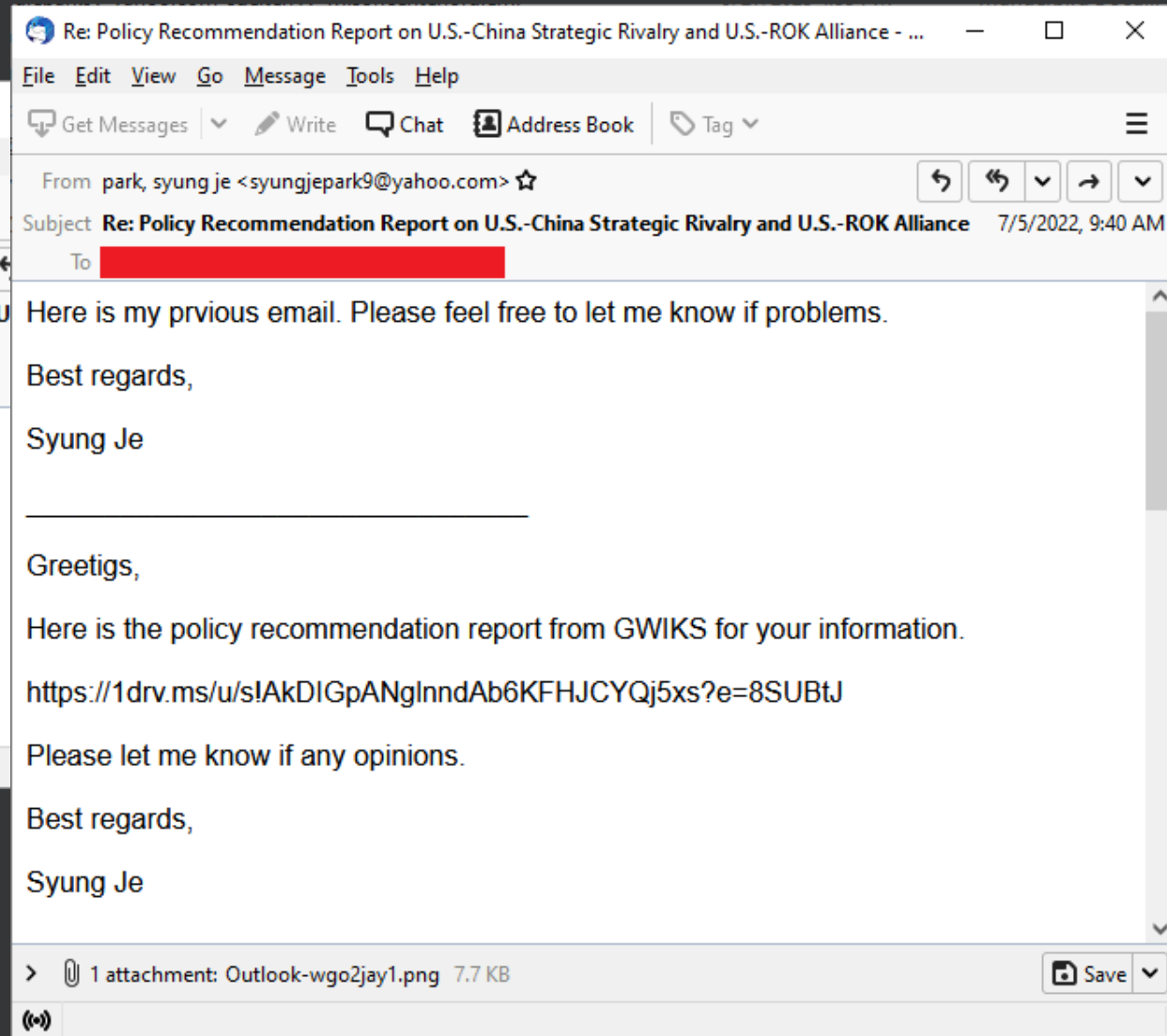
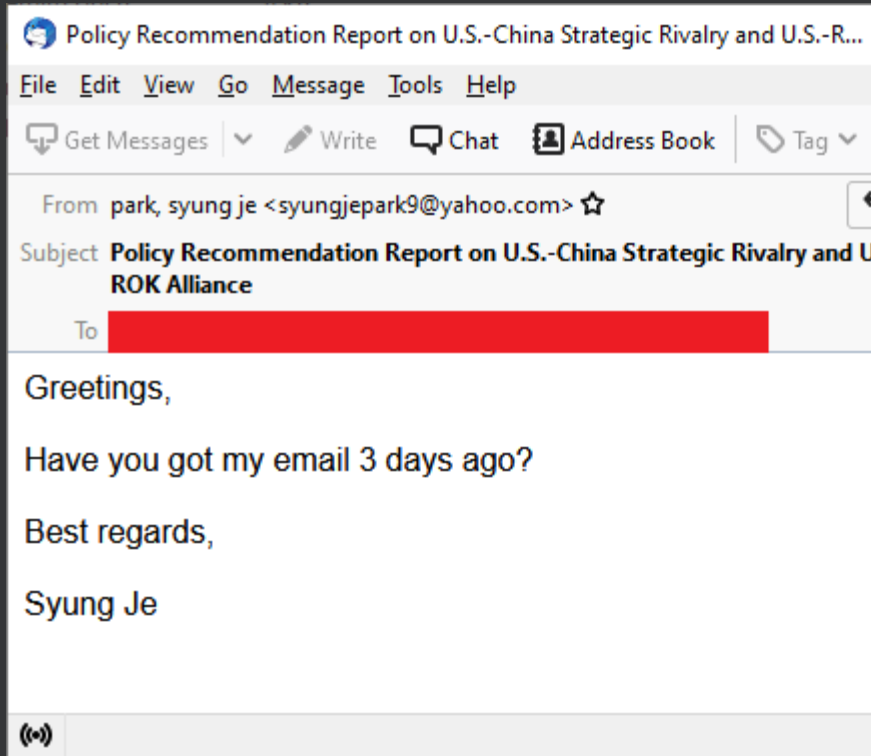


Key phishing principles

- Make the user feel **comfortable & secure**.
- Make the user feel **time-pressured** into opening the content.
- Now... for some examples.



Example #1: Sharing a Document



Example #2: Submit to My Conference

From: Yeowon Lim <dslkde@yahoo.com>
Sent: Wednesday, September 30, 2020 9:23 PM
To: [REDACTED]
Subject: Invitation Letter for a Paper of Special Edition from International Journal of Korean Unification Studies

Dear Sir,
Hello, this is Yeowon Lim, research associate at Korea Institute for National Unification (KINU) and editor of International Journal of Korean Unification Studies (JKUS).
On behalf of our Editor-in-Chief Dr. Bo-hyuk Suh, I am writing an email to extend you a formal invitation to write a paper of the special edition of our journal (submission deadline: November 21 and publication date: December 20, 2020). We are planning a special edition in marking the 70th anniversary of the Korean War this year and the feature theme of this edition is "Peaceful Transition from the Armistice Regime to a Peace Regime: In Commemoration of 70th Anniversary of the Korean War." Dr. Suh believes that you are best-equipped to write a paper for this particular subject.
Please find the attached Editor-in-Chief's letter for further details.
I look forward to your reply.
Sincerely,

Yeowon Lim

=====

Lim Yeowon

Research Associate & English Editor
International Journal of Korean Unification Studies
External Affairs and Public Relations Team
Korea Institute for National Unification

임여원 연구원 (영문논총 편집간사 & 영문에디터)
통일연구원 기획조정실 대외홍보팀

=====



Example #2: Submit to My Conference

Dear [REDACTED]

Thanks so much for accepting our invitation. We'd like to suggest you choose your paper's topic

Below link is our guideline and code of ethics for reference.

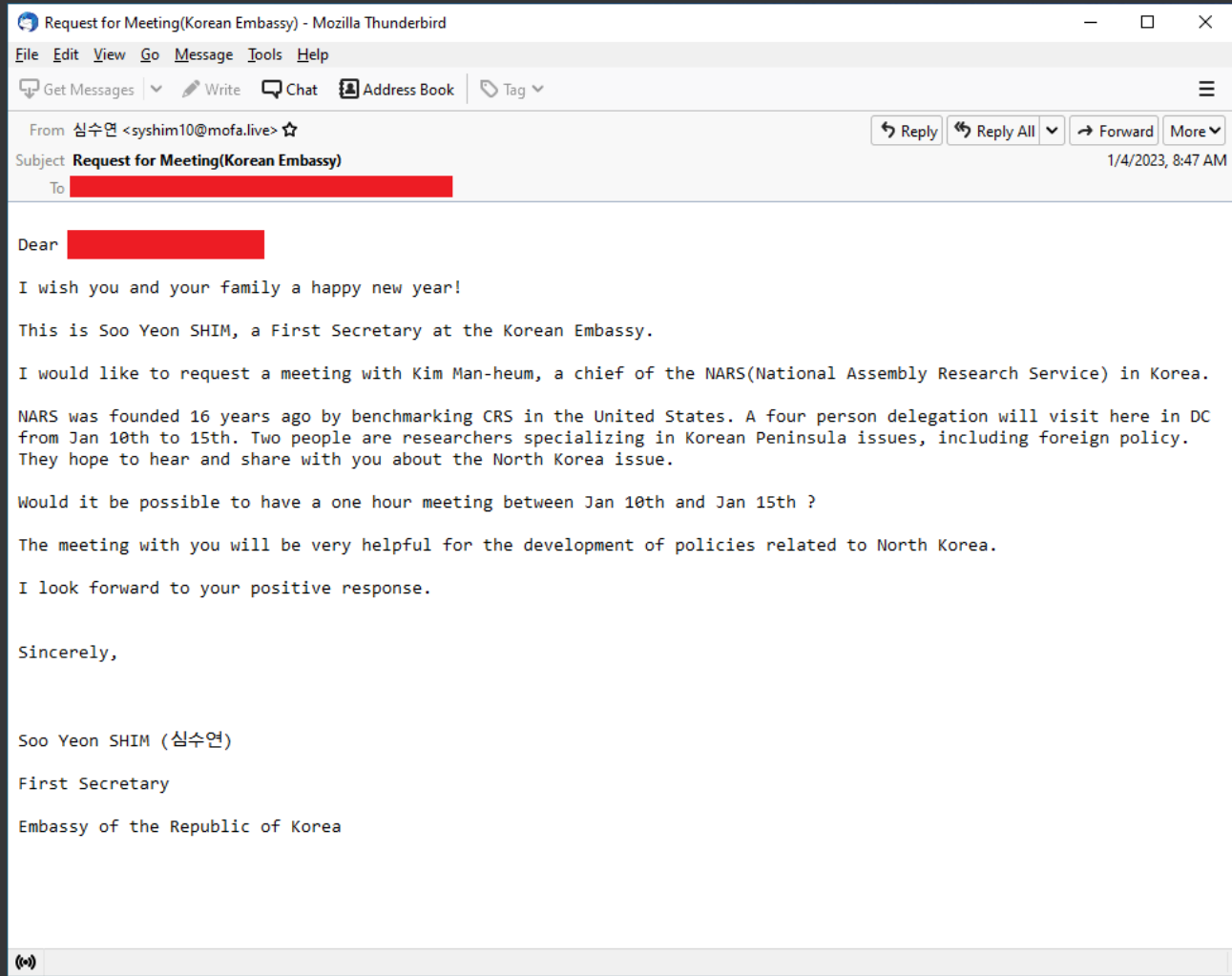
https://1drv.ms/u/s!AmK_4vZ8GWPqf5WAu4atuw2dsqw?e=Nvvejd

pwd: il@388IJKUS#

- N.B. Password protecting content is SOP for newer phishing content from SharpPine

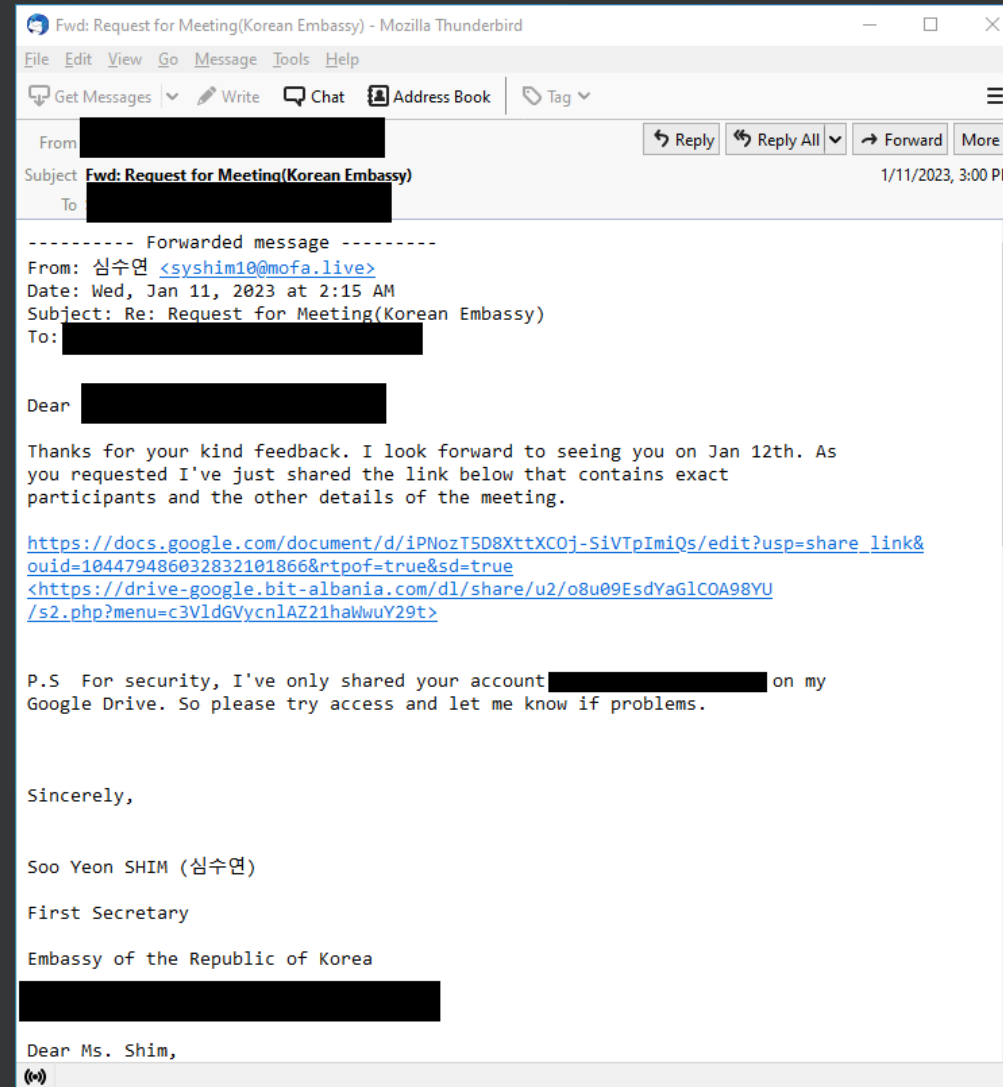
Example #3: Let's Meet Up

- I'm a government official at the Embassy!
- I'd like to request a meeting with the chief of a Korean Government service.
- Please propose a date!



Example #3: Let's Meet Up

- They agree a time and place.
- Target asks about other participants.
- **JUST ONE DAY before the meetup:** Attacker sends a link to a fake Google Drive link.



Example #4: Please Write a Paper

- Hey I'm a researcher @ the Sejong Institute
- Could you please write a 1200-word piece for our website on China-DPRK relations by August 19th?

Dear [REDACTED]

This is WOO Jung-Yeop, research fellow at the Sejong Institute, Korea.
I would like to ask whether you will be able to write a 1,200 words piece=
for our website, www.koreaonpoint.org

We launched the website last Friday to share diverse views on Korea quest=
ions.

The subject I ask you is
As it looks like China and DPRK is once again strengthening their ties in=
cluding border trade and food aid,

- Do you think China will expand its trade and/or aid to DPRK?
- Is China a facilitator or spoiler to bring DPRK back to negotiations wi=
th the US?
- Why do you believe so? (depending on your answer to the questions above=
)

You can send me to this email by Aug 19.
You can make your own title for your article.

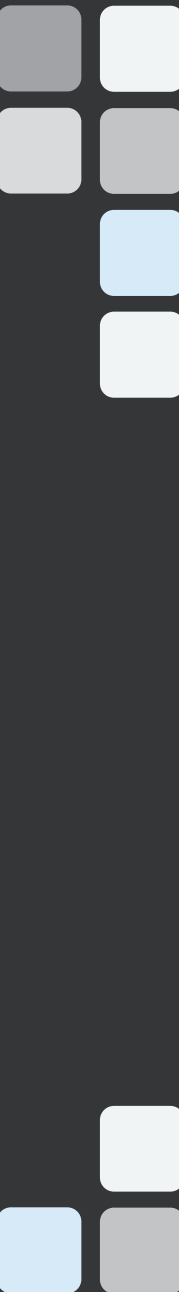
If you can visit our website, you will see what that is about.
We can provide you with the small honorarium of around USD 480.00.

I would really appreciate if you can contribute.

all the best,

Jung-Yeop

WOO Jung-Yeop



Example #4: Please Write a Paper

Dear [TRUNCATED],

Thanks for your response. I did review this and modify a bit.

<https://1drv.ms/u/s!As5EEMQwLFF>

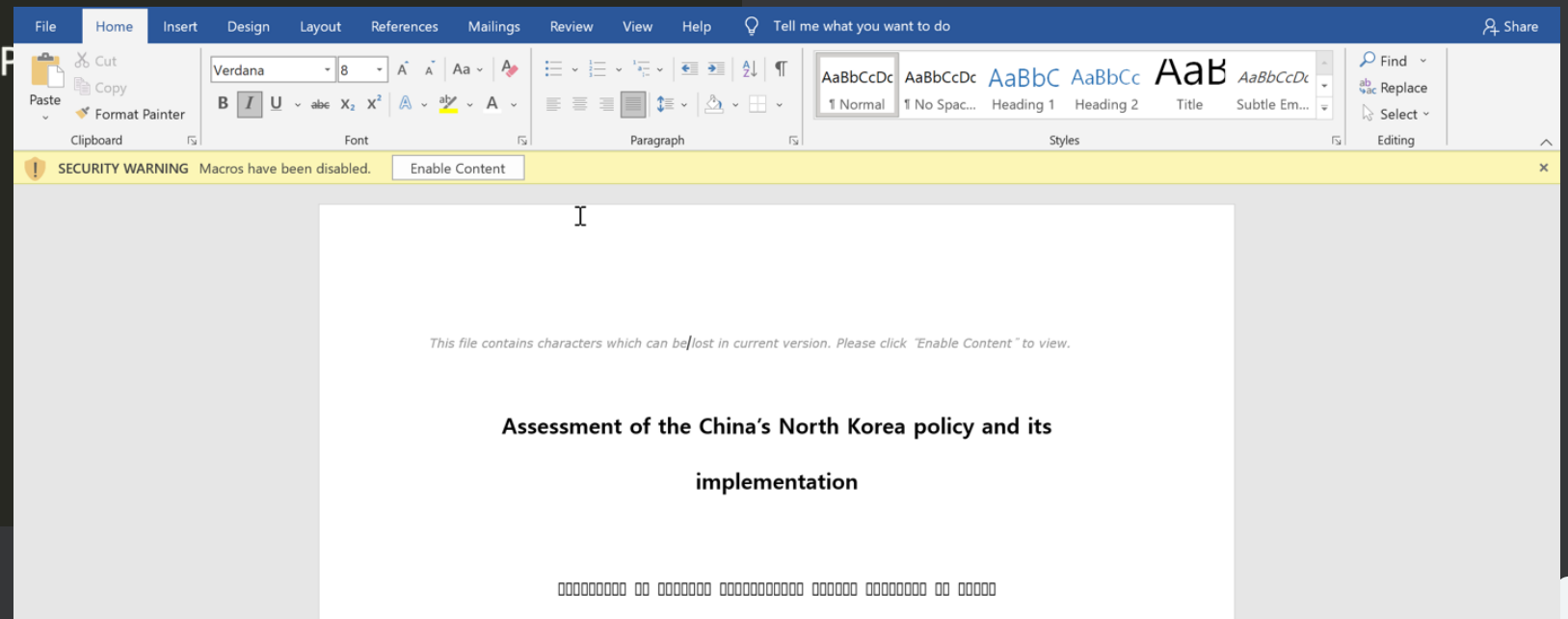
PW: WJY1030#@!

Please let me know if you have

all the best,

Jung-Yeop

W00 Jung-Yeop



Workflow recap (Examples: 1-4)

- User gets asked to do something they normally do for work.
- User does that thing
- User gets content back from the attacker
- User gets pwned if they enable content 😞



Example #5: Secure Your Account (!)

Hi Tim,

Thanks for your query.

Recently, there have been ~~login attempts~~ from other locations stealing NKPRO users' account information. Therefore, we've decided to re-register the IP area of NKPRO users to prevent illegal use. (<https://www.nknews.org/ip/register/>)

We hope for the active cooperation of NK PRO Account users. If not, you could have any problems in using NK PRO after updating the service.

All the best,

Melanie

--

Account Manager

membership@nknews.pro

Book a demo of NK Pro

**Non-existent
page on real
NKNews site.**



Example #5: Secure Your Account (!)

Hi Tim,

So sorry for my mistakes. I was very busy yesterday. So I'd like to resend the link (IP-register).

<https://nknews.org/2023/ip/register/>

Please log in NK PRO and register as soon as possible.

Thanks for your consideration and time again.

P.S If you log in successfully, registration is completed automatically.

All the best,

Melanie

**Phishing
page for
"nknews
Pro"(RTF)**



Example #5: Secure Your Account (!)

Hi Tim,

Sorry for troubling you, And thanks for your advice.

So, as a countermeasure, I would like to register your account(ip) myself.

Please send me your current id , pw and ip (NKpro login)so that I can complete it.

Then, I'll inform you soon after finishing. Please let me know if any problems.

Thanks for your consideration and time again.

All the best,

Melanie

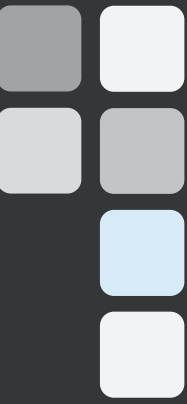
--

Account Manager

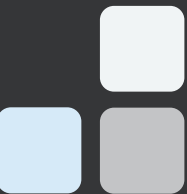
membership@nknews.pro

Book a demo of NK Pro





Infrastructure



Current* Infrastructure Trends

- Infrastructure habits change over time
- Different clusters*:
 - Previous (2021 and prior):
 - Compromised infrastructure
 - GMO Server (JP)
 - Current favourite: NameCheap + free TLD (often)
- Organization impersonation:
 - stimson\.pro
 - nknews\.pro



STIMSON

NK★NEWS



2019 C2 Management

- In 2019 Volexity worked with a compromised website to monitor SharpPine activity for a period of one month.
- We were able to monitor the operations of the attacker in real time.
- Eventually the website owner wanted to clean up. **Volexity notified all compromised individuals observed.**



2019 C2 Management: Logging

- Requests made to the root URL were logged.
- Attacker would periodically review visiting IP addresses // user agent and manually ban them

```
<?php
header("Expires: Mon, 26 Jul 1997 05:00:00 GMT"); // Date in the past
header("Last-Modified: " . gmdate("D, d M Y H:i:s") . "GMT"); // always modified
header("Cache-Control: no-store, no-cache, must-revalidate"); // HTTP/1.1
header("Cache-Control: post-check=0, pre-check=0", false);
header("Pragma: no-cache"); // HTTP/1.0
date_default_timezone_set('America/New_York');
$ip = getenv("REMOTE_ADDR");
$Now_time = time();
$date = date("Y/m/d h-i-s-A", $Now_time);
$useragent = isset($_SERVER['HTTP_USER_AGENT']) ? $_SERVER['HTTP_USER_AGENT'] : "";

if($ff=fopen("resp_suspect","a"))
{
    fwrite($ff, $date . " " . $ip . " suspected access " . $useragent . "\r\n");
    fclose($ff);
}
header('Location: http://go.microsoft.com/');
exit;
?>
```

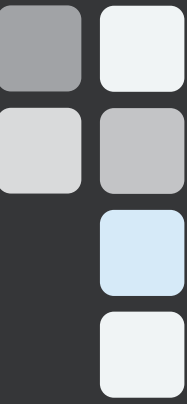
2019 C2 Management: Banned Response

```
// this is for wild card matches
foreach($bannedIP as $ip0) {
    if(preg_match('/' . $ip0 . '/', $_SERVER['REMOTE_ADDR'])){
        header('HTTP/1.0 404 Not Found');
        if($fff=fopen("resp_suspect","a"))
        {
            fwrite($fff, $date . " " . $ip . " suspected access " . "\r\n");
            fclose($fff);
        }
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
    }
}
}
```

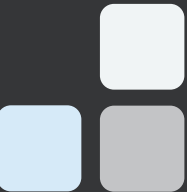
2019 C2 Management: help.txt

- Attacker would manually upload files to the C2 using a webshell. Typically, all files for any attack deployed as a ZIP and decompressed on the server side.
- Alongside the actual malware there was often "help.txt" – containing instructions on how to use the files.
- Suggests developer of malware != operator.





Malware



BABYSHARK

- Documented by Palo Alto Networks in 2019.
- Generally used to refer to a myriad of different scripts which share an encoding function

```
7  Function Decxe(c)
8      d = 8:
9      lsuh = Len(c):
10     strbax = "":
11     For jxgfq = 0 To d - 1:
12         For ixbnq = 0 To Int(lsuh / d) - 1:
13             strbax = strbax + Right(Left(c, ixbnq * d + jxgfq + 1), 1):
14         Next:
15     Next:
16     strbax = strbax + Right(c, lsuh - Int(lsuh / d) * d):
17     Decxe = strbax
18 End Function
```

BABYSHARK

- Taking an input string "hello world"
- Transposes it, using a distance of "3"

	A	B	C
1	h	l	w
2	e	o	o
3	l		r



Remaining text 'ld'
is appended

Hlweool rld



On ONE compromised device... (Jun 2022)

- **Five (!)** one-liner script malware samples on disk.
 - Run an arbitrary remote HTA x2.
 - Run a VBScript stored in the registry -> Fetches another VBScript.
 - Run an arbitrary file stored at a GoogleDrive URL.
 - Run an arbitrary remote PowerShell script.
- MISSDAISY (simple downloader DLL malware)
- SHARPEXT



SHARPEXT – Their Best Work

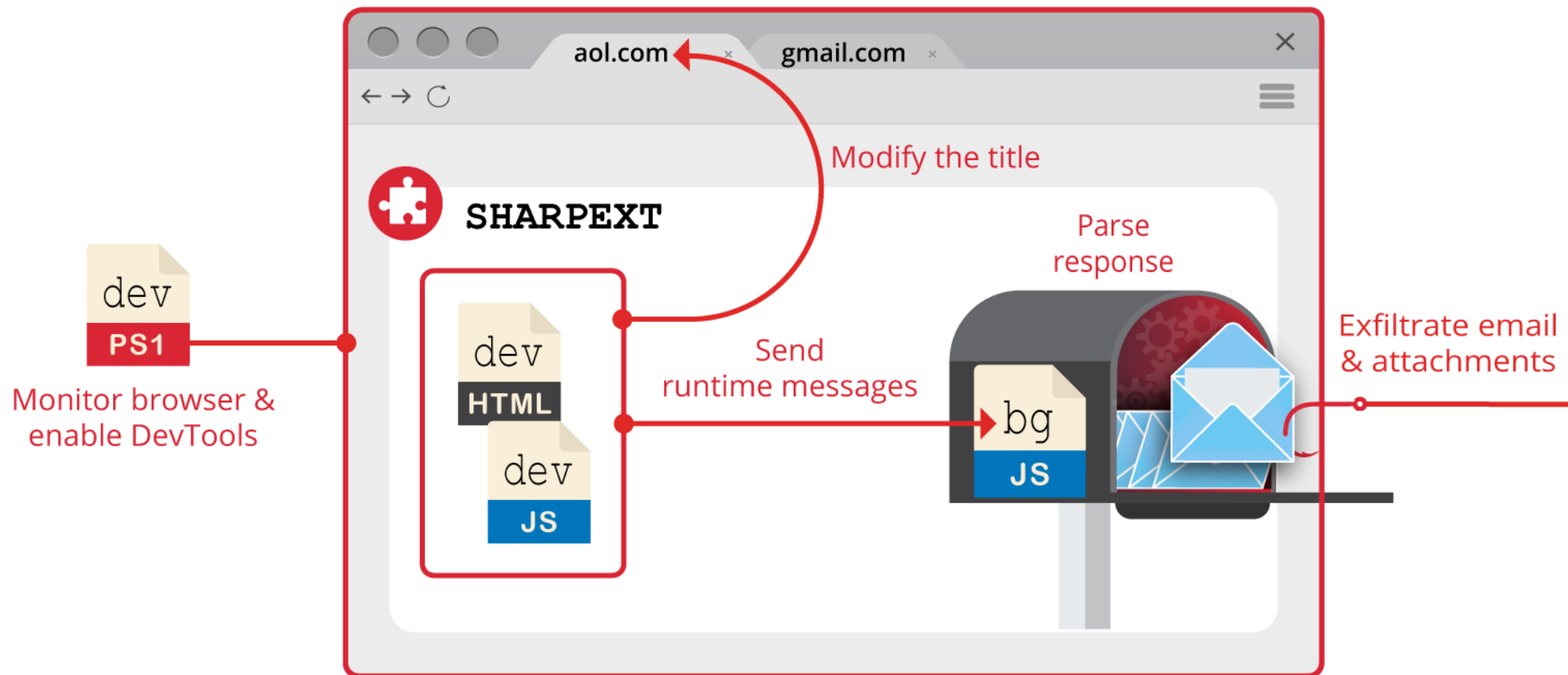
VOLEXITY // INTELLIGENCE

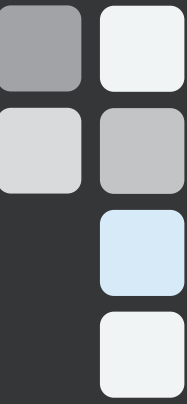
SharpTongue Deploys Clever Mail-Stealing Browser Extension "SHARPEXT"

- SharpTongue is a North Korean actor using newly discovered mail-theft malware, SHARPEXT
- Browser extension SHARPEXT steals mail data directly from webmail sessions
- Targeted users in USA, Europe, South Korea

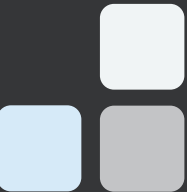


SHARPEXT – Their Best Work





Outlook



Putting the “P” in APT

- Once a target, always a target – you won’t fall off the list.
- May target the same individual multiple times per week.
- Willing to invest time in “the conversation” before trying to deliver any malware.



Conclusions

- Targeting of users' personal devices & email makes detection difficult
- A real risk in sectors where personal device use for work is common (media/NGO)
- Once a user is compromised, no automated solution will fix things
- Working closely with targeted organizations and users is key to mitigating this threat





Thank you for your time!

If you have any further questions or comments, feel free to reach out.

Contact

email: tlancaster@volexity.com

twitter (or is it X?): @tlansec

