Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks

By Anomali Threat Research

Published: 2025-12-18 · Archived: 2026-04-02 10:47:31 UTC

revised on August 22, 2019

Anomali researchers recently observed a site masquerading as a login page for a diplomatic portal linked to the French government. Further analysis of the threat actor's infrastructure uncovered a broader phishing campaign targeting three different countries' Ministry of Foreign Affairs agencies. Also targeted were four research-oriented organisations including: Stanford University, the Royal United Services Institute (RUSI), a United Kingdom-based think tank, Congressional Research Service (CRS), a United States-based think tank, and five different email service providers. There is an overlap of infrastructure with known North Korean actors, including the same domain and shared hosting provider. Because of the links between one of the victims and their work on North Korean sanctions, we expect to see malicious actors continue to target the international staff involved in a similar official capacity.

Prior to the release of this blog post, we have submitted the phishing sites to Google Safebrowsing and Microsoft for blacklist consideration.

Targeting of French Ministry of Europe and Foreign Affairs

On August 9, 2019, The Anomali Threat Research Team discovered a web page impersonating the French Ministry for Europe and Foreign Affairs (MEAE) online portal. The malicious host "portalis.diplomatie.gouv.fr.doc-view[.]work"[1] bears a strong resemblance to the legitimate site "diplomatie.gouv.fr". When navigating to the suspicious subdomain, users are displayed with a phishing site mimicking the MEAE portal. According to the legitimate site, access is restricted to "MEAE agents". The legitimate website for "France Diplomatie", describes MEAE agents as potentially working for one of 12 agencies for the "Ministry for Europe and Foreign Affairs". If an official from any of these agencies is able to login to the portal, then it is possible that all twelve of these agencies are potential victims, which includes:

- Agence Française de Développement (AFD)
- Agency for French Education Abroad (AEFE)
- Agricultural Research Centre for International Development (CIRAD)
- Atout France
- Business France
- Campus France and France Médias Monde
- Canal France International (CFI)
- Expertise France
- France Volontaires

- Institut Français
- Research Institute for Development (IRD)


Figure 1 - Faux login page for the portal of the Ministry of Europe and Foreign Affairs (MEAE)

The screenshot above shows the webpage designed to look like the MEAE portal. The screenshot shows a session timeout popup window for the victim who has attempted to login. In this instance, although not visibly clear, the page source shows the intended victim. This person was most likely targeted in a phishing campaign.

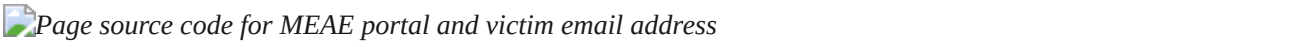


Figure 2 - Page source code for MEAE portal and victim email address

The email in the page source code is for an employee of the target organisation. According to delegefrance[.]org, the email address in the page source code belongs to a senior official assigned to the French Mission Team to the United Nations in New York. Moreover, this French diplomat works in the “Disarmament, Non-Proliferation, Sanctions committees: Iran, North Korea, 1st Committee”.[2]

Threat Infrastructure Analysis

The malicious URL “portalis.diplomatie.gouv.fr.doc-view[.]work” is mimicking a diplomatic portal on the malicious domain “doc-view[.]work”. This domain is hosted on the IP 157.7.184[.]15 and has several subdomains that appear to be designed to impersonate email providers. The IP address also appears to have several similar domains and URLs that share some patterns in naming conventions.


Figure 3 - Similar named domains hosted on the same IP address

The IP address 157.7.184[.]15 is hosted by the Asia Pacific Network Information Centre (APNIC). There are multiple unrelated domains hosted on the same IP address because the IP address is shared. The IP is based in Japan and registered under the Japan Network Information Centre located in Tokyo.

The most recently used domains on this IP address that share the same naming conventions are the following four domains:

Domain 1 - doc-view[.]work

The domain doc-view[.]work is hosted on IP 157.7.184[.]15. The domain has 32 subdomains.[3] Most of the subdomains appear to be spoofing email service providers Yahoo, Outlook, Ymail and Google services. Both the domain and some of the subdomains appear to have been set up to look like they will allow the victim to access documents; the use of Microsoft OneDrive for example.

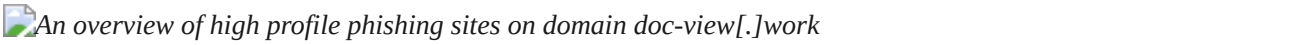
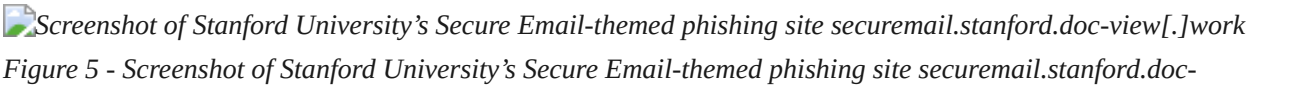


Figure 4 - An overview of high profile phishing sites on domain doc-view[.]work

Figure 4 above depicts the most interesting subdomains created for the domain doc-view[.]work to include two subdomains set up to impersonate the MEAE login. We also identified a subdomain "securemail.stanford.doc-view[.]work" created by the malicious actor to mimic Stanford University's Secure Email service.[4] According to Stanford University IT Department's website, the Secure Email service is designed for faculty and staff who need to use email to send moderate or high risk data. Of note, Stanford University hosts the Centre for International Security and Cooperation (CISAC) and the Asia Pacific Research Centre (APARC) - both of which are part of the Freeman Spogli Institute for International Studies. These research centres host a number of talks and deliver research on a variety of international issues including ongoing developments in North Korea.


Screenshot of Stanford University's Secure Email-themed phishing site securemail.stanford.doc-view[.]work
Figure 5 - Screenshot of Stanford University's Secure Email-themed phishing site securemail.stanford.doc-view[.]work

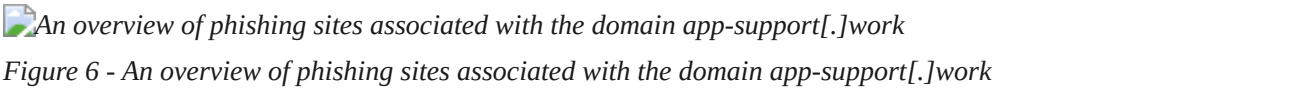
The submitted URL in URLScan.io, an online service for scanning and analyzing websites, shows the potential victim in the screenshot available, confirms the target institute as being Stanford University. A search in the Stanford Directory did not reveal anyone associated with this email address at Stanford University.

When investigating SSL/TLS certificates issued for the domain doc-view[.]work, there were five other fraudulent subdomains spoofing two think tanks, two foreign government agencies, and a United Nations organization.

- Congressional Research Service, a United States-based think tank
- Ministry of Foreign and European Affairs of the Slovak Republic
- Ministry of Foreign Affairs - Unknown country
- Royal United Services Institute (RUSI), a United Kingdom-based think tank
- South African Department of International Relations and Cooperation
- United Nations delegation

Domain 2. app-support[.]work

The domain app-support[.]work is hosted on the same IP address 157.7.184[.]15. The domain has a number of subdomains that look like they are attempting to impersonate popular email providers such as Yahoo and Gmail. The use of the domain "app-support" suggests the campaigns associated with this domain may be targeting smart-phones or Apple devices, because of the use of the word "app".


An overview of phishing sites associated with the domain app-support[.]work
Figure 6 - An overview of phishing sites associated with the domain app-support[.]work

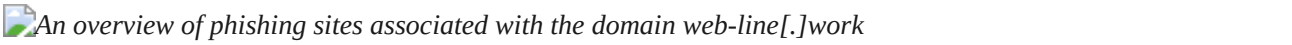
High profile targets in the above diagram include:

- Sina - A Chinese technology company

Domain 3. web-line[.]work

The domain web-line[.]work is hosted on the IP 157.7.184[.]15. The domain has a number of subdomains that appear to be mimicking well-known online services such as Google's Gmail and Microsoft's OneDrive. Interestingly, the domain owner also created a seemingly identical MEAE-themed subdomain

“portalis.diplomatie.gouv.web-line[.]work” that presumably attempts to mimic the MEAE portal. At the time of this report, the website was unresponsive; therefore, we were unable to obtain a screenshot of the page or analyze the site’s source code. Due to the domain name and infrastructure similarities of the original discovery, we judge with moderate confidence that the second subdomain was most likely created to target MEAE using the same techniques discussed above.


An overview of phishing sites associated with the domain web-line[.]work
Figure 7 - An overview of phishing sites associated with the domain web-line[.]work

In Figure 7, we highlight several high profile organizations targeted by the attackers. The following list reflects the most interesting targets in the overview of subdomains:

- Mail.fed.be - possible attempt to target the Federal government of Belgium
- Ministry of Europe and Foreign Affairs - France (MEAE)
- Ministry of Foreign Affairs (MOFA) - unknown country
- Sina - a Chinese technology company
- The Department of International Relations and Cooperation - The foreign ministry of the South African government

Domain 4. sub-state[.]work

When investigating passive DNS results on the same IP address 157.7.184[.]15, the domain “sub-state[.]work” was discovered. This domain has ten subdomains that follow the same naming conventions as the ones mentioned already.


An overview of phishing sites hosted on domain sub-state[.]work
Figure 8 - An overview of phishing sites hosted on domain sub-state[.]work

In Figure 8 it is possible to see subdomains impersonating the following organisations:

- Asahi News organisation - one of five major newspapers in Japan
- Ministry of Foreign Affairs - South Korea

Who’s Behind These Attacks?

The IP address 157.7.184[.]15 is shared and therefore home to both legitimate and malicious activity. However, there is an overlap in infrastructure in a recent North Korean campaign called “Smoke Screen” reported on by ESTSecurity in April 2019[5]. The domain “bigwnet[.]com” was reportedly used as a command and control (C2) for the Kimsuky Babyshark network trojan, which is also hosted on the same IP address. Kimsuky Babyshark network trojan is associated with North Korea.

According to DomainWatch, an online service that collects domain registrant information, there is a registrant email address that appears to link a number of the aforementioned domains: ringken1983[at]gmail.com.[6]


Whois information for the domain doc-view[.]work
Figure 9 - Whois information for the domain doc-view[.]work

DomainWatch also shows that the following domains are also registered with the same email address:

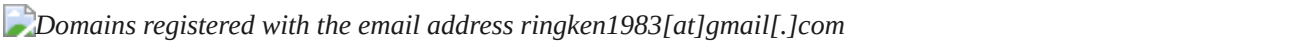


Figure 10 - Domains registered with the email address ringken1983[at]gmail[.]com

There are two other registrant emails identified for two related domains; “web-line[.]work” and “drog-service[.]com”.


Figure 11 - Domains registered with email address dragon1988[at]india[.]com

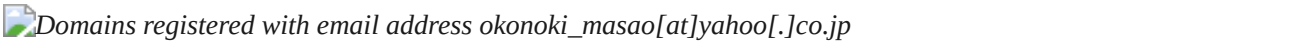


Figure 12 - Domains registered with email address okonoki_masao[at]yahoo[.]co.jp

The domain “Dauum[.]net” appears to be mimicking the South Korean web portal, Daum, which is an email provider among other services. In January 2019, North Korean actors were reported to have been targeting the Daum, Naver, and kakaoTalk services (all popular South Korean services), registering a number of similar-looking domains.[7]

Conclusion

Many of the organisations targeted in this campaign offer insight for strategic direction and goals of a particular country (South Korea for example). The targeting of foreign ministries for four different countries, and the persistent attempt to masquerade as email or online document services is most likely to gain access to the victim’s sensitive communications and/or information. The purpose of this campaign is likely to gain access to the information, but it is difficult to know exactly what the end goal is for the adversary. After gaining access to the internal email service of an organisation, it is possible to compromise the organisation in many other ways. Whilst researching this campaign, many of the domains were not active, although most were registered this year. It might be that the adversary has been waiting to use the infrastructure for a future attack. There is an overlap with North Korean indicators in this research, and similar targeting to previous campaigns already reported.

Endnotes

[1] URLScan, “portalis.diplomatie.gouv.web-line[.]work,” urlscan.io, accessed August 9, 2019, submitted July 23, 2019, https://urlscan.io/result/7e347bdc-8e0e-485b-93b2-6df2b919d768/.

[2] The French Mission Team, “Permanent mission of France to the United Nations in New York,” Ministry of Europe and Foerign Affairs, accessed August 12, 2019, https://onu.delegfrance.org/The-French-Mission-Team-8786.

[3] Censys, “doc-view[.]work,” Censys Certificate Search, accessed August 9, 2019, https://censys.io/certificates?q=%22doc-view.work%22.

[4] Stanford University, “Email:Secure Email: Email for Moderate and High Risk Data,” accessed August 14, 2019, published November 8, 2018, https://uit.stanford.edu/service/secureemail.

[5] Alyac, “Kimsuky’s APT Campaign ‘Smoke Screen’ Revealed for Korea and US,” ESTsecurity, accessed August 14, 2019, published April 17, 2019, https://blog.alyac.co.kr/2243.

[6] DomainWatch, “doc-view[.]work,” DomainWatch WhoIs, accessed August 12, 2019, https://domainwat.ch/whois/doc-view.work.

[7] BRI, “#1267555: Konni Campaign Targetting Mobiles - Additional IOCs,” BRI Alert, accessed August 14, 2019, published July 15, 2019, https://brica.de/alerts/alert/public/1267555/konni-campaign-targetting-mobiles-additional-iocs/.

Appendix A - Indicators of Compromise

The table below represents the malicious infrastructure and basic description of each indicator of compromise observed in the phishing campaign:

Indicators of Compromise	Description
157.7.184[.]15	Shared hosting server with multiple suspicious and phishing sites
doc-view[.]work	Malicious domain
web-line[.]work	Malicious domain
app-support[.]work	Malicious domain
login-confirm[.]work	Malicious domain
member-service[.]work	Malicious domain
short-line[.]work	Malicious domain
alone-service[.]work	Malicious domain
minner[.]work	Malicious domain
com-main[.]work	Malicious domain
sub-state[.]work	Malicious domain
check-up[.]work	Malicious domain
portalis.diplomatie.gouv.web-line[.]work	Phishing site mimicking the Ministry of Europe and Foriegn Affairs (MEAE) portal
account.googlie.com.doc-view[.]work	Phishing site
crsreports.congress.doc-view[.]work	Phishing site mimicking the Congressional Research Service

delegate.int.doc-view[.]work	Phishing site likely to be mimicking the United Nations delegate login
drive.google.doc-view[.]work	Phishing site
drive.storage.com.doc-view[.]work	Phishing site
drives.google.doc-view[.]work	Phishing site
hostmaster.doc-view[.]work	Phishing site
login-history.doc-view[.]work	Phishing site
login-onedrive.doc-view[.]work	Phishing site
login.live.doc-view[.]work	Phishing site
login.outlook.doc-view[.]work	Phishing site
login.yahoo-sec.doc-view[.]work	Phishing site
login.yahoo.doc-view[.]work	Phishing site
login.ymail.doc-view[.]work	Phishing site
mail.doc-view[.]work	Phishing site
mail.mofa.gov.doc-view[.]work	Phishing site mimicking the Ministry of Foriegn Affairs (MOFA) - unknown country
mail.preview.doc-view[.]work	Phishing site
mail.sec.doc-view[.]work	Phishing site
mail.view.doc-view[.]work	Phishing site
mail.xmailgateway.doc-view[.]work	Phishing site
myaccount.google.doc-view[.]work	Phishing site
myaccount.protect.doc-view[.]work	Phishing site
myaccount.setting.doc-view[.]work	Phishing site
mzv.sk.doc-view[.]work	Phishing site mimicking the Ministry of Foreign and European Affairs of the Slovak Republic
one-drive.storage.doc-view[.]work	Phishing site
onedrive.com.doc-view[.]work	Phishing site

portalis.diplomatie.gouv.doc-view[.]work	Phishing site mimicking the Ministry of Europe and Foriegn Affairs (MEAE) portal
portalis.diplomatie.gouv.fr.doc-view[.]work	Phishing site mimicking the Ministry of Europe and Foriegn Affairs (MEAE) portal
rusi.org.doc-view[.]work	Phishing site mimicking the UK think tank RUSI
securemail.stanford.doc-view[.]work	Phishing site mimicking Stanford University
ubmail.dirco.gov.doc-view[.]work	Phishing site mimicking the Department of International Relations and Cooperation of the Foreign Ministry of the South African government
www.str8-creative.com.doc-view[.]work	Phishing site
rive.storage.com.doc-view[.]work	Phishing site
login.yalnoo-sec.doc-view[.]work	Phishing site
login.onedrive-storage.doc-view[.]work	Phishing site
david.gizmodo.com.doc-view[.]work	Phishing site
drive.storage.login-confirm[.]work	Phishing site
share.doc.login-confirm[.]work	Phishing site
accounts.live.com.member-service[.]work	Phishing site
accounts.msn.com.member-service[.]work	Phishing site
accounts.outlooks.com.member-service[.]work	Phishing site
ccounts.outlooks.com.member-service[.]work	Phishing site
edit.accounts.member-service[.]work	Phishing site
maii.ocn-accounts.member-service[.]work	Phishing site
mail.ocn-accounts.member-service[.]work	Phishing site

login.outlook.short-line[.]work	Phishing site
1drv.ms.web-line[.]work	Phishing site
drive.storage.com.web-line[.]work	Phishing site
hostingemail.digitalspace.web-line[.]work	Phishing site
login.live.web-line[.]work	Phishing site
mail.fed.be.web-line[.]work	Phishing site
mail.mofa.gov.web-line[.]work	Phishing site
mail.xmailgateway.web-line[.]work	Phishing site
portalis.diplomatie.gouv.web-line[.]work	Phishing site
ubmail.dirco.gov.web-line[.]work	Phishing site
edit-accounts.ntt-ocn.alone-service[.]work	Phishing site
login-accounts.yahoojp.minner[.]work	Phishing site
login-accounts.yaoojp.minner[.]work	Phishing site
login.live.com-main[.]work	Phishing site
login.ymail.com-main[.]work	Phishing site
mail.mofa.go.kr.sub-state[.]work	Phishing site
accounts.ocn-setting.app-support[.]work	Phishing site
login-accounts.view.app-support[.]work	Phishing site
login.yahoo.app-support[.]work	Phishing site
loing-accounts.view.app-support[.]work	Phishing site
myaccount.google-monitor.app-support[.]work	Phishing site

myaccounts.google-set.app-support[.]work	Phishing site
vip-sina.com.cn.app-support[.]work	Phishing site
accounts.lives.com.check-up[.]work	Phishing site
accounts.msn.com.check-up[.]work	Phishing site
accounts.outlookes.check-up[.]work	Phishing site
accounts.outlooks.check-up[.]work	Phishing site
lh.yahoojp.check-up[.]work	Phishing site
mail.ocn-accounts.check-up[.]work	Phishing site
ringken1983[at]gmail[.]com	Adversary email address used to register domains
dragon1988[at]india[.]com	Adversary email address used to register domains
okonoki_masao[at]yahoo[.]co[.]jp	Adversary email address used to register domains

For more information, contact Joe Franscella: jfranscella@anomali.com

---