월간 악성코드 분석 보고서 (2018-03)

평창올림픽 파괴 악성코드 분석 보고서

수산INT 기술 연구소 (CERT)

2018. 03. 09

2018년 평창동계올림픽과 개막식에서 발생한 악성코드를 분석한 보고서 입니다.
본 문서는 수산아이앤티 CERT에서 작성되었으며 연구 목적의 활용은 가능하나, 그 외 활용으로 인해 발생하는 문제에 대한 법적 책임은 당사자에 있음을 알려드립니다.

문의처: 기술 연구소 CERT (SungMin.Rue@soosan.co.kr / KimNamGuy@soosan.co.kr)

SOOSAN INT

목 차

1. 개 요

2월 9일에 평창 동계 올림픽이 개막되었고, 25일에 폐막식과 함께 끝이 났습니다. 개막식 때 발생한 사이버 공격만 빼면 동계 올림픽을 성공적으로 마무리가 되었다고 볼 수 있는데요. 개막식 당일 평창 올림픽을 방해할 목적으로 사이버 공격이 발생하여, 동계 올림픽 관련 웹 사이트 마비. 올림픽 현장에서 와이파이 서비스 중단, 미디어센터 IPTV가 중단되는 등의 사고가 잇따랐습니다[1]. 다행히 다음날 10일 오전 8시에 정상 복구가 돼 평창 동계 올림픽 진행에는 큰 문제가 없었습니다.

이번 사이버 공격에는 국가 기관이 배후에 있는 것으로 추정하고 있는데요. 러시아가 이번 공격 배후로 가장 많이 거론되고 있습니다. 초기에는 북한의 소행으로 간주했지만, 사이버 공격 행위를 분석한 결과 러시아 해커 그룹과 유사한 징후가 많이 포착되었습니다. 특히 작년 우크라이나를 대상으로 배포한 악성코드 낫페트야 (Notpetya)와 유사점이 많이 발견되었습니다. 결국, 러시아가 북한 소행으로 위장해 사이버 공격으로 벌인 것으로 추정할 수 있습니다.

국내에서는 '파괴형 악성코드', 해외에서는 올림픽 디스트로이어 (Olympic Destroyer)로 명명되고 있는데, 이름에서 알 수 있듯이 시스템 파괴용 목적으로 제작됐다는 것을 알 수 있습니다. 실제로 악성 실행 파일 모두 시스템 파괴용 목적으로 제작돼 있었습니다. 이는 올림픽을 방해하기 위한 목적으로 만들어졌다는 것을 더욱더 확신케 하는 것으로 볼 수 있습니다.

저희 CERT 파트에서는 해당 악성코드가 올림픽 방해용으로 만들어졌다고 해도 간과해서는 안 되는 악성코드로 결론을 내렸습니다. 다른 분야에 응용돼 활용될 수 있음은 물론이고, 복구할 수 없을 만큼 시스템에 치명적인 악영향을 미치기 때문입니다. 따라서 "평창올림픽 파괴형 악성코드" 주제로 본 보고서를 작성했습니다. 순서는 다음과 같습니다.

2 장에서는 평창올림픽에서 일어난 사이버 공격 내용을 시작으로 배후로 추정되는 조직과 유사 공격 기법을 살펴볼 예정입니다. 그리고 3장에서는 실제로 저희 CERT 파트가 분석한 악성코드의 행위를 소개하고, 이에 대응할 수 있는 방안을 제안하고자 합니다.

---

1) 전자신문 (보도일: 2018. 02. 13), "평창올림픽 사이버 공격... 국가 조직 해커가 시스템 파괴 시도", http://www.etnews.com/20180213000318

2. 올림픽 파괴형 악성코드

2월 9일 평창 올림픽을 방해할 목적의 사이버 공격으로 인해 와이파이 서비스, 미디어센터 IPTV가 중단되는 등의 사고가 잇따랐습니다. 다행히 다음날인 10일 오전 8시에 정상 복구가 되어 올림픽 진행에는 큰 피해가 가지 않았습니다.

해당 악성코드는 시스템 복구가 불가능할 정도로 강력한 파괴력을 가지고 있어, 국내에서는 '파괴형 악성코드', 해외에서는 '올림픽 디스트로이어'로 명명되었는데요. 초기에는 IP 등이 북한과 연관된 것으로 보여, 북한을 이번 사이버 공격 배후로 지목했습니다. 그러나 미국 정찰국 (US Intelligence)은 러시아 해외 정찰국 (GRU)이 평창 올림픽을 대상으로 사이버 공격을 벌인 것으로 잠재 결론을 내렸습니다[2]. 이른바 러시아가 북한이 공격한 것으로 위장한 "위장 술책 작전 (False Flag Operation)"을 수행한 것입니다.

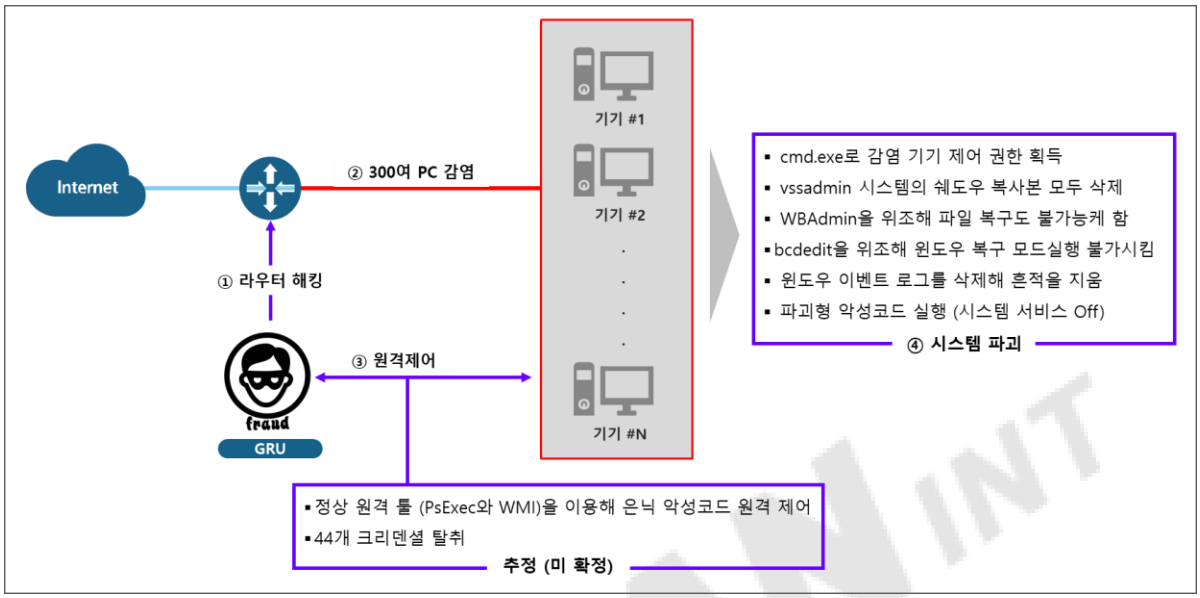
러시아가 평창 올림픽을 대상으로 사이버 공격을 벌일 만한 동기는 충분합니다. 이번 평창 올림픽에 참전이 금지된 것이 가장 큰 동기로 볼 수 있습니다. GRU가 벌였다는 증거도 포착됐습니다. 파괴형 악성코드에서 낫페트야와 유사한 특징들이 발견됐기 때문입니다. 참고로 낫페트야는 2017년에 우크라이나의 주요 기관을 공격한 랜섬웨어 악성코드로, 러시아를 배후로 지목하고 있습니다. 아울러 1월에 GRU로 의심되는 기관이 한국의 평창 올림픽 관련 라우터 서버를 해킹하고 개막식 바로 전날 악성코드를 심는 행위도 포착되어, GRU가 이 같은 공격을 벌였다는 주장을 더욱더 명확하게 하고 있습니다.

따라서 이번 장에서는 시스코가 분석한 평창 올림픽 사이버 공격 내용과 GRU가 벌인 낫페트야 공격을 살펴보도록 하겠습니다.

2) Washington Post (2018), "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say".

2.1 평창 올림픽 사이버 공격 사건 내용[3)]

아래 그림은 시스코에서 제공한 분석 정보와 추가 조사 자료를 기반으로 평창에서 이용한 파괴형 악성코드 공격 과정을 도식화한 것입니다.



러시아의 GRU로 추정되는 그룹이 지난 1월에 한국의 라우터를 해킹한 것으로 밝혀졌습니다. 워싱턴 포스트에 따르면, 이후 올림픽 조직위원회와 관련된 300여 대의 컴퓨터 기기의 권한을 탈취했습니다. 만일 GRU가 평창 올림픽을 정말로 공격했다면, 44개 크리덴셜 (Credential)[4)] 탈취 과정은 300여 대 컴퓨터 기기 권한 탈취 과정에서 일어났다고 볼 수 있지요.

시스코 탈로스 분석에 따르면, 해당 기기에 접근하기 위한 수단으로는 정상 원격 툴 (PsExec와 WMI)를 사용했는데요. 이는 정상적인 접근으로 위장해 보안 검열을 우회하기 위함 입니다. 또한 크리덴셜 탈취를 위해서 두 개의 악성코드가 사용된 것으로 드러났습니다. 브라우저 크리덴셜 스틸러 (Browser Credential Stealer)는 브라우저상의 크리덴셜을

3) Talos (2018), "Olympic Destroyer Aim At Winter Olympics", https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

4) 특정 응용에서 사용하는 암호학적 개인 정보를 뜻함.

탈취하는 악성코드로, 크롬, 파이어폭스, 익스플로러를 지원합니다. 시스템 크리덴셜 스틸러는 시스템의 크리덴셜을 탈취하기 위한 악성코드로, 주로 LSASS[5]에 있는 크리덴셜을 얻으려는 시도가 눈에 띄었습니다.

앞서 언급했듯이, GRU가 배후라면 개막식 당일 전에 삽입한 악성코드는 파괴형 악성코드일 확률이 높습니다. 크리덴셜 탈취 후 목표 서버에 도달했을 때 공격을 위한 파괴형 악성코드의 경우 복구가 거의 힘들게 하는 악성 행위들이 눈에 많이 띄었습니다. cmd.exe로 명령을 주로 내리는데, 우선 vssadmin 시스템의 쉐도우 복사본을 모두 삭제해 파일 등의 복구를 불가능하게 했습니다. 또한 WBAdmin을 공격해 파일 손상 복구를 하지 못하게 했고, 시동 구성 데이터 (Boot Configuration Data) 에 사용하는 bcdebit을 건드려 부팅에서 복구하는 것 또한 못하게 막고 있습니다. 추가로 윈도우 로그에 흔적을 지워서 공격자가 누구인지를 밝히지 못하게도 했습니다. 이러한 과정 이후에 최종적으로 시스템을 공격해 서비스를 동작하지 못하도록 만들어 버립니다.

해당 악성코드의 목적 자체가 복구 불가능하게 시스템을 파괴 하는 것입니다. 그리고 평창 올림픽 관련 서버를 노린 것으로 보아, 명백히 평창 올림픽 방해 목적을 위해 만든 것으로 보입니다.

2.2 러시아 정찰국과 낫페트야

시스코의 분석에 따르면, 평창 올림픽 파괴형 악성코드는 낫페트야 (NotPetya) 악성코드와 유사합니다[6]. 실제로 파괴형 악성코드를 분석한 결과, 피해 기기를 원격 제어할 때 사용하는 툴 (PsExec와 WMI)이 낫페트야 때와 유사했습니다. 아울러 크리덴셜을 탈취할 때

5) LSASS (Local Security Authority Subsystem Service): 보안정책 강화를 위해 비밀번호 변경을 관리하는 윈도우의 하위 시스템.

6) Forbes (FEB 12, 2018), "This 'Olympic Destroyer' Malware May Have Killed Winter Games Computers", https://www.forbes.com/sites/thomasbrewster/2018/02/12/winter-olympics-cyberattack-and-the-destroyer-malware/#5a042db937e4

파이프 코드 함수[7]를 사용 하는 것도 발견했는데요. 이 또한 낫페트야에서 보이는 특징입니다. 참고로 낫페트야는 우크라이나를 대상으로 공격한 랜섬웨어형 악성코드로, 1,700여 대의 기기가 감염된 것으로 조사됐습니다. 다른 국가들도 피해를 보았는데요. 항만회사 머스크 (Maersk)의 경우, 낫페트야로 최소 2,000억 원의 피해를 보았습니다. 미 정보국 (CIA)는 지난 우크라이나 발전시설을 공격한 블랙에너지와 유사한 것을 고려해 러시아가 낫페트야 배후국가로 잠재 결론을 내렸습니다[8]. 우크라이나 보안청 (SBU)도 러시아를 배후국으로 지목했으며, 영국의 경우 러시아가 낫페트야를 벌인 것에 대해 강하게 비난하기도 했습니다[9].

파괴형 악성코드가 낫페트야와 유사하다는 점과 낫페트야 배후국가가 러시아라는 점을 고려했을 때, 저희 CERT팀은 러시아가 파괴형 악성코드라고 잠재 결론을 내릴 수 있게 되었습니다. 특히 러시아로부터 평창 올림픽 이전의 악성 공격 증후가 관찰됐다는 점을 고려하면, 러시아가 이 같은 악성 공격을 벌였을 가능성이 높은 것으로 판단했습니다. 동기 또한 명확하다고 볼 수 있습니다.

지금까지 평창 올림픽 개막전에 발생한 사이버 공격 분석 내용을 살펴보았습니다. 정리하면 다음과 같습니다.

1. 파괴형 악성코드는 복구를 불가능하게 한 다음 시스템을 파괴하기 때문에 매우 위험합니다.
2. 낫페트야와 유사한 공격으로, 러시아가 배후 국가일 가능성이 매우 높습니다.

---

7) 파이프 (Pipe): 유닉스 계열에 사용하는 함수로, 정보를 전달하는 명령을 내릴 때 사용 됨.

8) Washington Post (JAN 12, 2018), "Washington Post: Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes", https://www.kyivpost.com/ukraine-politics/washington-post-russian-military-behind-notpetya-cyberattack-ukraine-cia-concludes.html

9) TechCruncgh (FEB 15, 2018), "UK accuses Russia of 2017's NotPetya ransomware attacks", https://techcrunch.com/2018/02/15/uk-accuses-russia-of-2017s-notpetya-ransomware-attacks/

3. 분석 내용 (Olympic Destroyer)

수산INT CERT에서는 파괴형 악성코드를 실제로 분석해 보았습니다. 분석 내용을 다음과 같습니다.

3.1 분석 파일 정보

분석 파일명은 "**Olympic Malware.exe**" 입니다.

해당 파일 해쉬 정보는 아래와 같습니다.

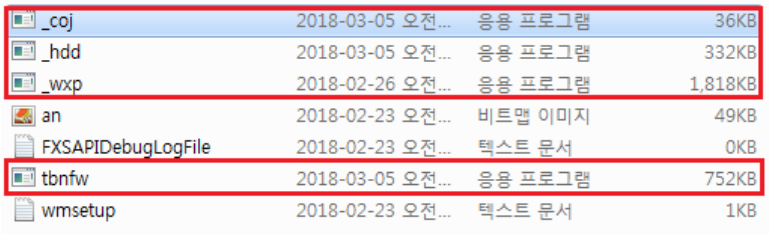
- MD5: fb519776cad0114763f417c4344e4be9
- SHA-1: 6e0345705620f7803e2ac6ccdf82db035e66d444
- SHA-256: dc5e401c53b6ca8a92d72e6fbecea52f6ef9d45c1e8d53902a6f674ea7f9ee16

아울러 테이블에서 보는 것과 같이, 여러 파일들이 드롭 (악성파일 등을 심는 행위) 되는 것을 발견했습니다.

드롭 파일명	파일의 악성행위
Copy Olympic Malware.exe	Olympic Malware.exe의 복사본
Browser Stealer.exe	브라우저 정보 탈취
Psexec.exe	원격 제어 파일
Olympic Destroyer.exe	시스템 파괴를 목적으로 한 핵심 악성 파일

3.2 실행증상 (동적분석)

Olympic Malware의 주 기능은 브라우저 스틸, 원격 프로그램, 시스템 파괴 파일들을 Drop 하는데 있습니다. 그 중에서 원격 프로그램 Psexec는 정상 프로그램이며, 단순히 원격 기능이 사용 가능한 점을 악용하는데 이용 하였습니다. 이 원격 기능으로 프로세스 간 통신하면서 시스템 내부를 파괴하거나, 컴퓨터 주요 정보를 탈취 시도를 하는 행위가 보였습니다. 그리고 Drop 될 때의 파일명은 랜덤으로 생성이 되면 순서대로 생성 됩니다.



[드롭 된 파일]

첫번째 드롭파일 (올림픽 멀웨어 파일 드롭 실행 코드)

```
00407271 .  E8 CACDFFFF          CALL 평창_edb.00404040

Stack address=0012E708, (ASCII "C:\\Users\\an\\AppData\\Local\\Temp\\_wxp.exe")
EAX=00000001
```

두번째 드롭파일 (Browser Stealer 파일 드롭 실행 코드)

```
00407266 .  E8 35F3FFFF          CALL 평창_edb.004065A0

0012D88C  007C6278  UNICODE "C:\\Users\\an\\AppData\\Local\\Temp\\tbnfw.exe"
0012D890  778FE0ED  ntdll.778FE0ED
```

세번째 드롭파일 (원격제어 "Psexec" 파일 드롭 실행 코드)

```
00407299 .  E8 92CCFFFF          CALL 평창_edb.00403F30

0012E13C  0012E308  ASCII "C:\\Users\\an\\AppData\\Local\\Temp\\_hdd.exe"
```

네번째 드롭파일 (Olympic Destroyer 파일 드롭 실행 코드)

```
004072AD .  E8 7ECCFFFF          CALL 평창_edb.00403F30

0012E13C  0012EB08  ASCII "C:\\Users\\an\\AppData\\Local\\Temp\\_coj.exe"
0012E140  DFFBE031
0012E144  DFE91F01
```

그리고 해당 악성 파일에서 특이한 점을 찾아 냈습니다. 바로 기존에 있던 "스위프트(SWIFT) 악성코드[10]"랑 유사한 단어가 존재 했다는 것입니다. 실질적으론 해당 경로 "%Programdata%₩evtchk.txt"에는 "evtchk.txt" 라는 파일은 존재하지 않습니다. 하지만 SWIFT 악성코드에서는 evtchk.bat, evtdiag.exe, evtsys.exe 라는 악성 파일을 사용 했었고 해당 파일 이름이 존재 하는 걸로 보아 스위프트 악성코드를 제작한 라자라스 그룹[11]의 하위 조직인 블루노로프(Bluenoroff) 집단이 제작 한 것 일수도 있다는 추측이 나왔었습니다. 그러나 미국 정보국의 분석 결과를 고려하면, 앞서 언급했듯이 이러한 행위는 북한이 악성공격을 한 것처럼 보이기 위한 위장 술책 작전인 것으로 보입니다.

```
ASCII "%d.%d.%d.%d"
UNICODE "cmd.exe /c (ping 0.0.0.0 > nul) && if exist %programdata%\\evtchk.txt (exit 5) else ( type nul > %pro"
UNICODE "del %programdata%\\evtchk.txt"
ASCII "invalid vector<T> subscript"
```

[evtchk 파일명]

10) 북한과 연관 있는 것으로 추정되는 최상위 해킹 그룹

11) 방글라데시의 SWIFT 기관을 노려 1,000억원 가량을 탈취한 악성공격

3.2.1 Olympic Malware

- 우선 실행 파일 Olympic Malware.exe 의 자기 자신을 복제하여 _wxp.exe 라는 이름으로 파일을 만듭니다. 그리고 프로세스 간의 통신을 할 수 있는 PIPE 함수를 사용하여 “123” 이라고, 파이프 명명 합니다.

```
0012D868  0012D8A0  UNICODE " 123 \\\\.\\pipe\\B0E2D5F6-3EC6-45FA-8B75-C12CF8D7405B"
0012D86C  00424BA8  UNICODE " %ls %ls"
0012D870  00424C08  UNICODE "123"
0012D874  0012DEA0  UNICODE "\\\\.\\pipe\\B0E2D5F6-3EC6-45FA-8B75-C12CF8D7405B"
```

- Psexec 원격 제어 프로그램과 통신을 전송 할 명령어 및 WMI 명령어로 컴퓨터의 정보나 프로세스 정보 등을 얻어 올 수 있습니다.

```
UNICODE "Win32_Process"
UNICODE "cmd.exe /c (echo strPath = Wscript.ScriptFullName & echo.Set FSO = CreateObject^(\"Scripting.FileSyst"
UNICODE "CommandLine"
UNICODE "\\\\%s\\root\\CIMV2"
ASCII "Select * From Win32_ProcessStopTrace"
ASCII "WQL"
UNICODE "Create"
UNICODE "Win32_Process"
UNICODE "CommandLine"
```

- 그리고 평창 올림픽 홈페이지에 관련하여 접근하는 흔적도 보였습니다. 해당 정보는 도메인 이름, 아이디, 비밀번호가 코딩 되어 있는게 보였습니다.

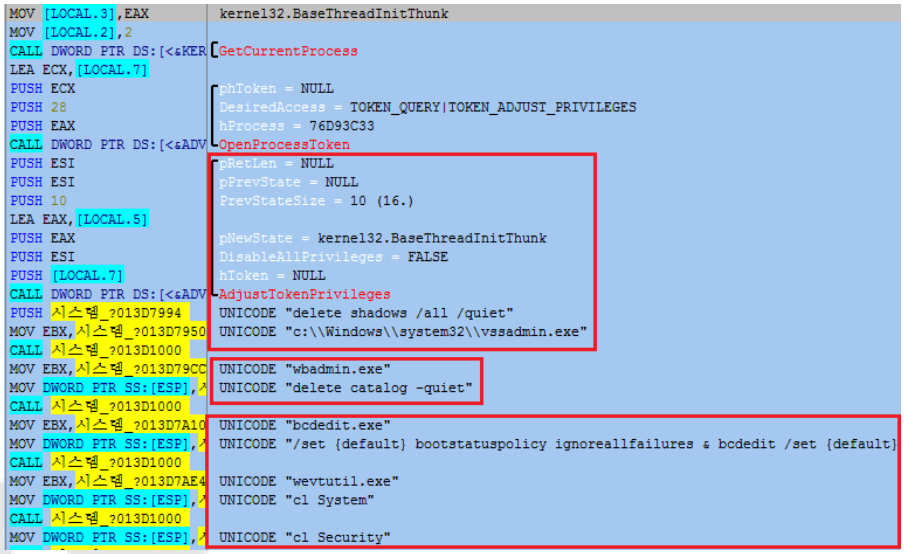
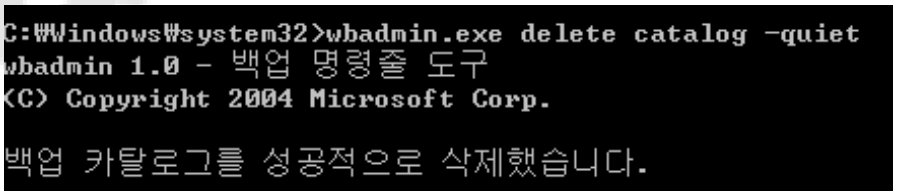
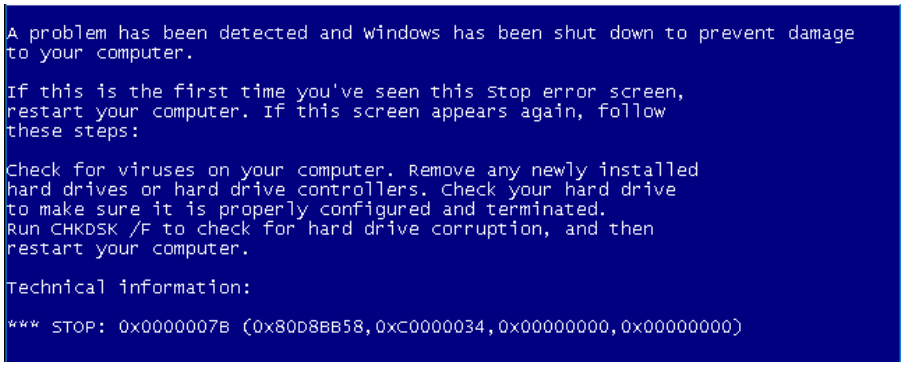
Address	Type	Value
0042691E	String[60]	Pyeongchang2018.com₩pcadmin
0042894B	String[60]	Pyeongchang2018.com₩PCA,GMSAdmin
0042897C	String[60]	Pyeongchang2018.com₩cert01
00428A24	String[60]	Pyeongchang2018.com₩PCA,lyncadmin
00428A5B	String[60]	Pyeongchang2018.com₩PCA,lyncadmintest
00428A96	String[60]	Pyeongchang2018.com₩PCA,SMSAdmin
00428AC7	String[60]	Pyeongchang2018.com₩addc,siem
00428AF3	String[60]	Pyeongchang2018.com₩jinsik,park
00428B21	String[60]	Pyeongchang2018.com₩pca,infradmin
00428B56	String[60]	Pyeongchang2018.com₩PCA,KASAdmin
00428B8B	String[60]	Pyeongchang2018.com₩PCA,OMEGAdmin
00428BBD	String[60]	Pyeongchang2018.com₩PCA,WEBAdmin
00428BF2	String[60]	Pyeongchang2018.com₩PCA,SDAdmin
00428C22	String[60]	Pyeongchang2018.com₩pca,sqladmin
00428C57	String[60]	Pyeongchang2018.com₩PCA,giwon,nam
00428C8A	String[60]	Pyeongchang2018.com₩svc_all_swd_installc
00428CC1	String[60]	Pyeongchang2018.com₩PCA,spsadmin
00428CF6	String[60]	Pyeongchang2018.com₩test
00428D1F	String[60]	Pyeongchang2018.com₩adm,pms
00428D4F	String[60]	Pyeongchang2018.com₩COS,SQLAdmin
00428D84	String[60]	Pyeongchang2018.com₩pca,dnsadmin
00428DB9	String[60]	Pyeongchang2018.com₩PCA,imadmin
00428DEC	String[60]	Pyeongchang2018.com₩pca,perfadmin
00428E1F	String[60]	Pyeongchang2018.com₩jaesang,jeong6
00428E52	String[60]	Pyeongchang2018.com₩pca,dnsadmin2
00428E84	String[60]	Pyeongchang2018.com₩pca,cpvpnadmin
00428EBA	String[60]	Pyeongchang2018.com₩pca,dmzadmin

```
address   EC ED EE EF F0 00 01 02 03 CDEF0123456789ABCDEF0123
00428FEC  50 79 65 6F 6E 70 6D 6F 5F Pyeongchang2018.com\pmo_
00429004  61 64 6D 69 6E 0B 00 50 79 admin.[illegible]Py
0042901C  65 6F 6E 67 63 6D 69 6E 00 eongchang2018.com\admin.
00429034  70 63 32 30 31 6E 67 63 68 [illegible]Pyeongch
0042904C  61 6E 67 32 30 6E 00 70 63 ang2018.com\web_admin.pc
00429064  32 30 31 38 31 63 68 61 6E [illegible]Pyeongchan
0042907C  67 32 30 31 38 70 63 32 30 g2018.com\cos_admin.[illegible]
00429094  31 38 31 32 33 61 6E 67 32 [illegible]Pyeongchang2
004290AC  30 31 38 2E 63 32 30 31 38 018.com\gms_admin.[illegible]
004290C4  31 32 33 34 21 67 32 30 31 [illegible]Pyeongchang201
004290DC  38 2E 63 6F 6D 71 77 65 31 8.com\lync.admin.c[illegible]
004290F4  32 33 24 00 1D 30 31 38 2E [illegible]Pyeongchang2018.
0042910C  63 6F 6D 5C 63 6D 69 6E 00 com\crm_admin.crm_[illegible]
```

[평창 관련 시스템 접근 계정]

3.2.2 Olympic Destroyer (시스템 파괴)

- 해당 명령어를 통하여 시스템 및 보안 이벤트 로그 삭제, Windows 복구 시스템 파괴 및 쉐도우 복사본, 백업 파일 삭제를 하여 부팅 시 컴퓨터가 제기능을 하지 못하도록 만들어 버리는 핵심적인 파일 입니다.
- 시스템 파괴 단계가 완성이 되면, 공격자의 입장에서 목표를 달성하였기에 공격은 성공적으로 이루어 진 거라 봅니다. 또 한 악성코드는 평창 올림픽 타겟으로 하며, 해당 인프라를 잘 알고 이용하여, 도메인 접근 및 공격을 한 걸로 보여집니다.

시스템 파괴 CMD 명령어	
시스템 파괴 명령어 실행 화면	
시스템이 파괴 된 화면	

3.3 대응방안

1. **eRed Hypervisor Security 설치로 파괴형 악성코드로부터 보호할 수 있습니다.**

   파괴형 악성코드는 서버를 대상으로 발생한 공격으로, 무서운 점은 복구가 불가능하게 만든 다음 시스템을 파괴 시킨 다는 것입니다. eRed는 파괴형 악성코드로부터 보호할 수 있습니다. 우선 비 권한 프로세스 실행 자체가 불가능하기 때문에, 분석 사례에서 설명한 악성행위 동작이 불가능 합니다. 이러한 차단 행위는 게스트 OS 하부의 하이퍼바이저 OS에 동작하기 때문에 파괴형 악성코드로부터 매우 안전하다고 할 수 있습니다.

2. **eWalker 설치로 감염을 예방할 수 있습니다.**

   파괴형 악성코드 유입 경로에 대해서는 아직 알려진 바가 없습니다. 다만 사이트를 감염시켜서 파괴형 악성코드와 같은 지능적인 악성코드를 배포하는 경우가 많습니다. 따라서 악성 사이트에 접속하지 않는 것 또한 가장 중요한 예방법이라고 할 수 있습니다. 그런데 문제는 악성 사이트를 탐지하는 것이 쉽지 않다는 것입니다. 자사에서 제공하는 eWalker 제품은 40만 개가 넘는 악성 URL을 보유하고 있습니다. 그러므로 사이트를 통한 감염을 최소화 시켜줄 수 있으므로, eWalker를 사용하는 것이 하나의 예방법으로 볼 수 있습니다.

3. **의심되는 메일을 열지 않는 것도 중요한 예방법입니다**.

   출처를 알 수 없는 메일에는 악성코드를 숨겨놓을 가능성이 높기 때문에, 의심메일을 열지 않는 것 또한 감염 사고 발생율을 줄일 수 있는 방법 입니다..

4. **백신과 OS를 정기적으로 업데이트 하는 것도 중요한 예방법입니다.**

   악성코드 감염 방지를 위해 백신과 OS를 정기적으로 업데이트하는 것도 중요합니다. 다만 알려지지 않은 악성코드인 경우 탐지가 힘듭니다. 이러한 경우 전문가 분석이 필요합니다. **본인이 속한 기관이 악성코드에 감염됐다고 의심된다면, 저희 보안 연구소에 연락 (QI@soosan.co.kr)을 주셔도 됩니다.**

2018 년 수산 INT 보안 연구 보고서 발간 내역

월간 악성코드 분석 보고서

2018-01 호: 가상화폐 채굴 악성코드 분석 (2018 년 01 월)
2018-02 호: UBoat Rat 분석 보고서 (2018 년 02 월)
2018-03 호: 평창올림픽 파괴 악성코드 분석 보고서 (2018 년 03 월)

감사합니다.

글로벌 네트워크 보안 솔루션 전문기업

SOOSAN INT

서울특별시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

Tel 02.541.0073 | **Fax** 02.541.0204

E-mail QI@soosan.co.kr

HP http://www.soosanint.com