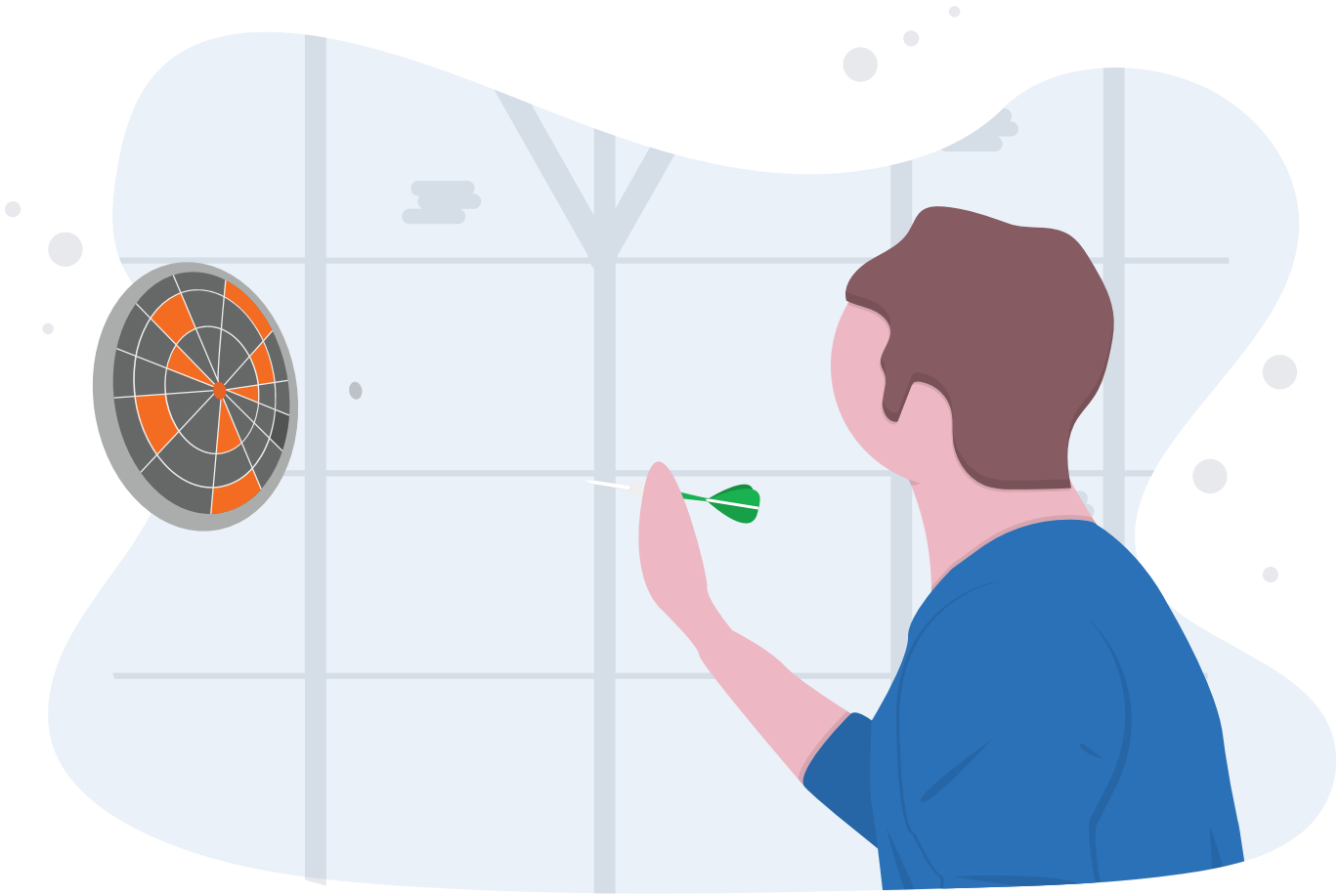
Recorded Future®

사이버 위협 분석

2019년 가장 많이 익스플로잇된 10대 취약점:

사이버 범죄의 인기 타겟은 여전히 Microsoft 제품

저자: Kathleen Kuczma, Briana Manalo



CTA-2020-0204

이 문서는 2019년 1월 1일부터 12월 31일까지 기간 동안 취약점 익스플로잇 키트, 피싱 공격, RAT(Remote Access Trojans) 발생 현황을 중점적으로 분석한다. 이를 위해 코드 리포지토리, 언더그라운드 포럼 게시판, 다크웹을 비롯한 수천 가지 소스가 분석되었다. 본 보고서는 2018년 보고서에 이어 후속 자료를 담고 있으며, 정보 보안 실무자(특히 취약성 위험 평가를 담당하는)에게 도움이 되는 정보를 제공한다.

요약

이 보고서는 2019년 지하 범죄 소스에서 가장 많이 익스플로잇된 취약점이 어떤 것들인지 분석한다. 레코디드 퓨처는 2018년과 마찬가지로 2019년에도 Adobe 제품에 비해 Microsoft 제품을 겨냥한 익스플로잇이 더 많음을 확인했다. 피싱 공격, 익스플로잇 키트, RAT(Remote Access Trojans)을 통해 익스플로잇된 취약점 10개 중8개가 Microsoft 제품에 영향을 주며, 그 중 4개가 Internet Explorer에 영향을 준다. Internet Explorer는 사용 감소 추세에도 불구하고 여전히 많은 기업 환경에서 실행되고 있는 최고의 공격 대상이다. Adobe Flash 취약점은 단 2개만이 상위 10위 안에 포함되었다. 이는 패치 강화와 2020년 하반기로 예정된 Flash Player 퇴출에 따른 결과이다.

많은 취약점/패치 관리팀이 사이버 범죄자들이 주로 노리는 취약점이 어떤 것인지 모른 채 셀 수 없이 많은 제품 패치 업데이트로 고군분투하고 있다. 이 작업이 얼마나 고된 것인지는 2019년에 보고된 CVE 취약점이 12,000개가 넘는다는 사실에서 잘 알 수 있다. 2018년 16,000개에 비하면 다소 줄었으나, 미국 정부와 NVD(National Vulnerability Database)는 이 12,000개 취약점 가운데 1,000개 이상을 CVSS 점수 9점 이상, 패치 “필수”로 분류했다.

CVE 데이터베이스와 기존 스캐닝 도구만으로는 조직 내 시스템들의 수많은 취약점 가운데 위협 행위자들의 주요 익스플로잇 대상이 되는 취약점이 무엇인지 알기 어렵다. 취약점의 패치 우선순위를 효과적으로 정하기 위해서는 무기화(Weaponization)에 대한 인사이트가 필요하다. 발견되자마자 1개월 또는 1년 이내에 무기화되는 취약점은 전체의 1%도 되지 않기 때문이다. 따라서 보안 담당자는 자사 기술 스택에 영향을 주면서 익스플로잇 키트에 포함되어 있거나, RAT 배포에 사용되거나, 피싱 공격에 사용되는 취약점에 대해 반드시 알고 있어야 한다.

주요 정보

- 3년 연속으로 Microsoft가 취약점의 영향을 가장 많이 받는 기술로 밝혀졌다. 2018년 보고서에서와 마찬가지로 상위 10개 취약점 중 8개가 Microsoft 제품을 겨냥한 것으로 확인되었다.
- Microsoft에 영향을 주는 6개 취약점이 전년도에 이어 10위권에서 동일한 순위를 유지했다. CVE-2018-8174는 2018년 가장 많이 익스플로잇된 취약점 1위에서 2019년에는 2위로 순위가 한 계단 하락했다. CVE-2017-11882는 그대로 3위에 머물렀으며, CVE-2012-0158은 9위에서 10위로 내려갔다.
- 2019년 10대 취약점 중 Internet Explorer 10 & 11에 영향을 준 취약점은 CVE-2019-0752 하나였다. 이 취약점은 Capesand라는 최신 익스플로잇 키트에 포함되었다.
- 최신 익스플로잇 키트 수가 계속 감소하여 2019년에는 5개에서 4개로 줄었다. Capesand는 이 목록의 취약점을 겨냥한 최신 익스플로잇 키트이다. 한 지하 포럼 사용자가 2019년 12월 Capesand와 DarkRat의 개발을 중단한다고 주장했다.
- 2019년에 23개의 최신 RAT(remote access trojan)이 등장했다. 2018년에 나온 것은 37개였다. 2019년 최신 RAT 가운데 상위 10대 취약점과 관련된 것은 단 하나이다. Microsoft WinRAR ACE에 영향을 주는 CVE-2018-20250를 겨냥한 BalkanRAT이 바로 그것이다.

Cyber Vulnerability	Company	Product	Associated Malware	CVSS	Recorded Future Risk Score
CVE-2018-15982	Adobe	Flash Player	Fallout Exploit Kit, Spelevo Exploit Kit, ThreadKit, GreenFlash Sundown, Lord Exploit Kit, GandCrab, Capesand Exploit Kit, Maze Ransomware	10	99
CVE-2018-8174	Microsoft	Internet Explorer	SLUB, Fallout Exploit Kit, Spelevo Exploit Kit, KaiXin Exploit Kit, LCG Kit Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Trickbot, Underminer Exploit Kit, Capesand Exploit Kit, Dridex, IcedID, Buran Ransomware, Gandcrab	7.6	99
CVE-2017-11882	Microsoft	Office	Agent Tesla Keylogger, Artemis, Formbook, Nanocore, PowerShower, Loki, Heur, Chanitor, Trillium Security MultiSploit Tool, Artemis, Emotet, Silent Doc Exploit, ThreadKit, VenomKit	9.3	99
CVE-2018-4878	Adobe	Flash Player	Gandcrab, Fallout Exploit Kit, RIG Exploit Kit, Spelevo, Capesand Exploit Kit, GreenFlash Exploit Kit, Hermes Ransomware, Sundown Exploit Kit, Threadkit Exploit Kit	7.5	99
CVE-2019-0752	Microsoft	Internet Explorer	SLUB, Capesand Exploit Kit	7.6	99
CVE-2017-0199	Microsoft	Office	njRAT, RevengeRAT, Pony, QuasarRAT, REMCOS RAT, SHUTTERSPEED, Silent Doc Exploit Kit, Threadkit Exploit Kit	9.3	99
CVE-2015-2419	Microsoft	Internet Explorer	Capesand Exploit Kit, Sundown Exploit Kit	9.3	99
CVE-2018-20250	Microsoft	WinRAR	BalkanRAT	6.8	99
CVE-2017-8750	Microsoft	Internet Explorer	ThreadKit Exploit Kit, QuasarRAT	7.6	99
CVE-2012-0158	Microsoft	Office	Silent Doc Exploit	9.3	99

2019년 가장 많이 익스플로잇된 상위 10대 취약점

배경

이전 년도와 마찬가지로 이 리스트의 목표는 다크웹 범죄에서 가장 많이 익스플로잇되는 취약점을 파악하는 것이다. 따라서 ETERNALBLUE와 같이 국가기관이 만든 익스플로잇과 관련된 취약점은 리스트에서 제외되었다. 레코디드 퓨처는 최근 수 년 간 Shadow Brokers와 같은 해커 그룹이 유출시킨 해킹 도구들이 다크웹 범죄의 익스플로잇 키트에 많이 사용되었거나 포함되었다는 증거는 확인하지 못했다.

레코디드 퓨처는 2019년 다크웹 범죄에서 가장 많이 익스플로잇된 취약점 중 상당수가 2018년에도 상위권 순위에 있었음을 확인했다. 상위 10위 내 취약점 중 6개가 전년도와 동일했다.

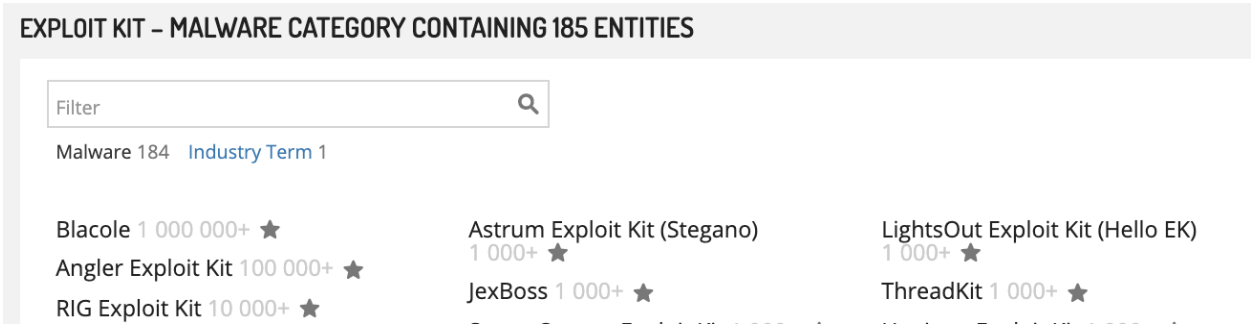
2019	2018	2017	2016
1. CVE-2018-15982	1. CVE-2018-8174	1. CVE-2017-0199	1. CVE-2016-0189
2. CVE-2018-8174	2. CVE-2018-4878	2. CVE-2016-0189	2. CVE-2016-1019
3. CVE-2017-11882	3. CVE-2017-11882	3. CVE-2017-0022	3. CVE-2016-4117
4. CVE-2018-4878	4. CVE-2017-8750	4. CVE-2016-7200	4. CVE-2015-8651
5. CVE-2019-0752	5. CVE-2017-0199	5. CVE-2016-7201	5. CVE-2016-0034
6. CVE-2017-0199	6. CVE-2016-0189	6. CVE-2015-8651	6. CVE-2016-1010
7. CVE-2015-2419	7. CVE-2017-8570	7. CVE-2014-6332	7. CVE-2014-4113
8. CVE-2018-20250	8. CVE-2018-8373	8. CVE-2016-4117	8. CVE-2015-8446
9. CVE-2017-8750	9. CVE-2012-0158	9. CVE-2016-1019	9. CVE-2016-3298
10. CVE-2012-0158	10. CVE-2015-1805	10. CVE-2017-0037	10. CVE-2015-7645

표: 2016년부터 2019년까지 가장 많이 익스플로잇된 CVE 리스트 (연속해서 상위권에 든 CVE는 색깔로 표시)

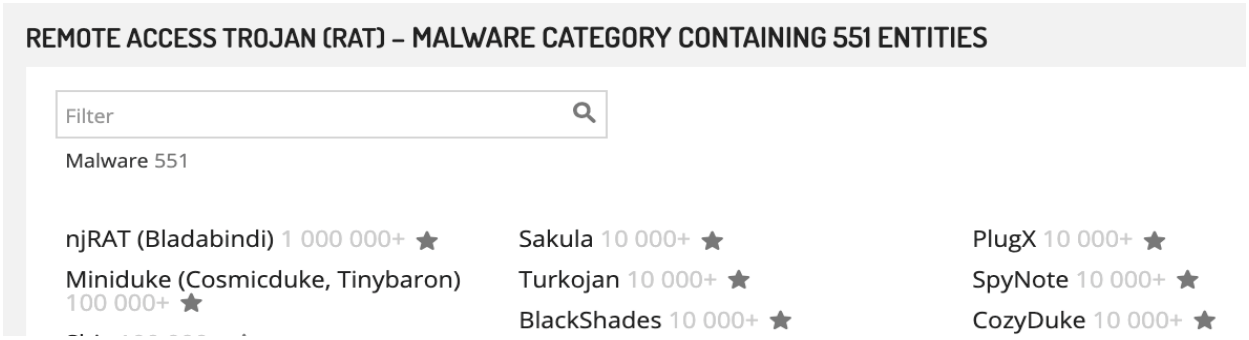
이 표에서 주목할 점은 CVE-2017-0199가 최근 3년 동안 익스플로잇순위에서 줄곧 최상위를 유지했다는 것이다.
이것은 CVE-2016-0189가 2018년 보고서에서 최초로 3년 연속 10대 취약점 리스트에 오른 데 이어 두번째이다. CVE-2017-0199는 ThreadKit 익스플로잇 키트에 포함되고 8가지 다른 종류의 멀웨어에 관련되어 2018년 5위에 올랐다. 2019년에도 10위권 안에 든 CVE-2017-0199는 여전히 빈번하게 악용되는 Microsoft 취약점이며, 언더그라운드 포럼에서 Silent Doc 익스플로잇 판매 광고가 계속되고 있다.

방법론 및 소스

이 보고서는 취약점과 익스플로잇 키트, RAT의 동시 발생 관계를 분석하고 추이를 파악한다. 레코디드 퓨처는 2019년 사이버 범죄에 가장많이 이용된 취약점을 파악하기 위한 매개변수 중 하나로 레코디드 퓨처 익스플로잇 키트 멀웨어 카테고리의 184개 익스플로잇 키트 리스트를 사용했다. 또한 레코디드 퓨처 RAT 멀웨어 카테고리 551개 RAT와의 관련성을 기반으로 가장 많이 악용되는 취약점 순위를 파악하였다.



레코디드 퓨처 익스플로잇 키트 멀웨어 카테고리



레코디드 퓨처 RAT 멀웨어 카테고리

ETERNALBLUE와 ETERNALROMANCE 익스플로잇 관련 취약점은 탑 10 목록에서 제외되었다. 이 두 개의 해킹툴은 다크웹 소스의 사이버 범죄 세계에서 주로 취급하는 것이 아니라 국가 사이버전에 속한 것이기 때문이다. ETERNALBLUE 익스플로잇(MS17-010 취약점 이용)과 ETERNALROMANCE(CVE-2017-0143 이용)는 언더그라운드 커뮤니티에서 자주 언급되지도, 익스플로잇 키트로 판매되지도 않았다.

ETERNALROMANCE(CVE-2017-0143)의 경우는 몇몇 언더그라운드 포럼 멤버들이 짧게 언급한 것이 전부이다. 이는 아마도 2017년 Shadow Brokers가 이 해킹툴들을 유출시켜 무료로 공개해버렸기 때문일 것이다. 게다가 ETERNALBLUE와 ETERNALROMANCE 익스플로잇은 사용이 간편하여 한때 널리 확산되었던 일반적인 익스플로잇 키트에 비해 훨씬 정교하고 사용 방법 또한 어렵다. 레코디드 퓨처의 이전 취약점 조사에서 알 수 있듯이 새로운 익스플로잇 키트의 출현은 계속 감소하고 있다. 그 이유는 강화된 브라우저 보안과 특정 피해자를 겨냥하는 표적 공격 때문이다.

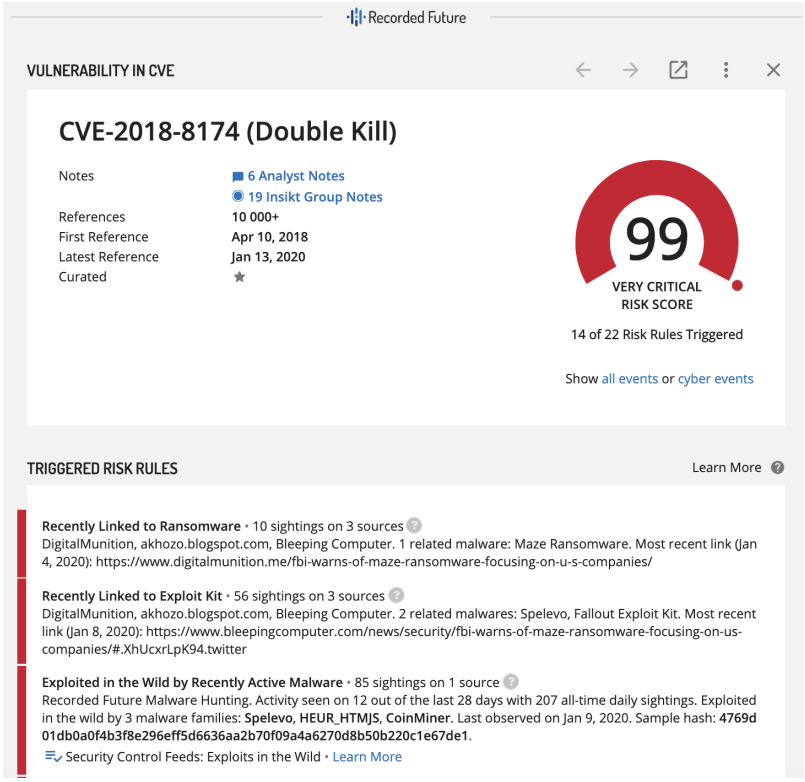
이 연례 보고서의 상위 10대 취약점 목록은 공개 소스와 비공개 소스 모두에서 수집한 정보의 데이터 분석 및 메타데이터 분석을 기반으로 한다. 레코디드 퓨처는 이 보고서에서 언급된 멀웨어에 대한 리버스 엔지니어링(Reverse-Engineer)을 실행하지 않았다. 이 보고서는 가장 많이 익스플로잇되는 취약점을 보여주는 데 목적이 있다.

익스플로잇 위험 점수 방법론

이 보고서는 위에서 설명한 방법론에 새로운 취약점 위험 점수 방법론을 결합했다. 레코디드 퓨처의 취약점 위험 점수(Risk Score)는 항상 무기화를 고려하여 산정된다. 레코디드 퓨처는 여기에 2019년 Insikt Group이 개발한 "Recorded Future Malware Hunting"을 공식적으로 추가하였다. 이 기능은 수십억 개의 멀웨어 샘플을 분석하여 그 중에서 보안팀이 주목해야 하는 정적/행동 특성을 가진 중요 샘플을 파악한다.

Malware Hunting의 서브셋인 "Exploits in the Wild" 데이터 세트[1]는 레코디드 퓨처가 최근 실제 환경에서 관찰한 멀웨어 활동에서 사용된 취약점을 찾아낸다. 이 데이터 세트는 주요 멀웨어 저장소의 샘플 제출 현황을 통해 실제 환경에서의 확산 정도를 가늠한다. 엔드포인트, 이메일, 네트워크에서 발견된 샘플을 멀웨어 저장소에 제출하는 작업이 대부분 보안 툴이나 안티바이러스 벤더에 의해 자동으로 수행되기 때문이다. 이 보고서에 소개된 가장 많이 익스플로잇된 상위 10대 취약점 모두가 이 위험 규칙(risk rule)을 따른다.

[1] 이 데이터 세트에 대한 자세한 사항은 Security Control Feeds의 이전 블로그 게시물을 참조할 것.



CVE-2018-8174에 대한 취약점 인텔리전스 카드(Vulnerability Intelligence Card). 위험 규칙 "Exploited in the Wild by Recently Active Malware" 포함.

가장 많이 익스플로잇된 취약점

2019년 가장 많이 익스플로잇된 취약점 1위는 CVE-2018-15982이다. 이 취약점은 2018년 목록에는 없었다. Adobe Flash Player 취약점 2개 중 하나인 CVE-2018-15982는 use-after-free 취약점이다. 즉, 이미 free한 메모리에 접근할 때 발생하는 버그이다. 이 취약점은 공격자가 악성 Flash 오브젝트를 피해자 시스템으로 전송하여 임의 코드를 실행할 수 있게 해준다. CVE-2018-15982는 2019년 최소 10개의 알려진 익스플로잇 키트(Fallout, Spelevo, GreenFlash, Sundown, Threadkit, Lord, RIG, UnderMiner, Capesand, Grandsoft)에 포함되었다. 레코디드 퓨처는 이 취약점을 2019년 가장 많이 익스플로잇된 취약점으로 평가한다. 다수의 유명 익스플로잇 키트에 포함되어 있기 때문이다. 이 취약점은 2019년 3월 21일 XSS Forum의 사용자 "ExploitCVE"에 의해 판매되었다.

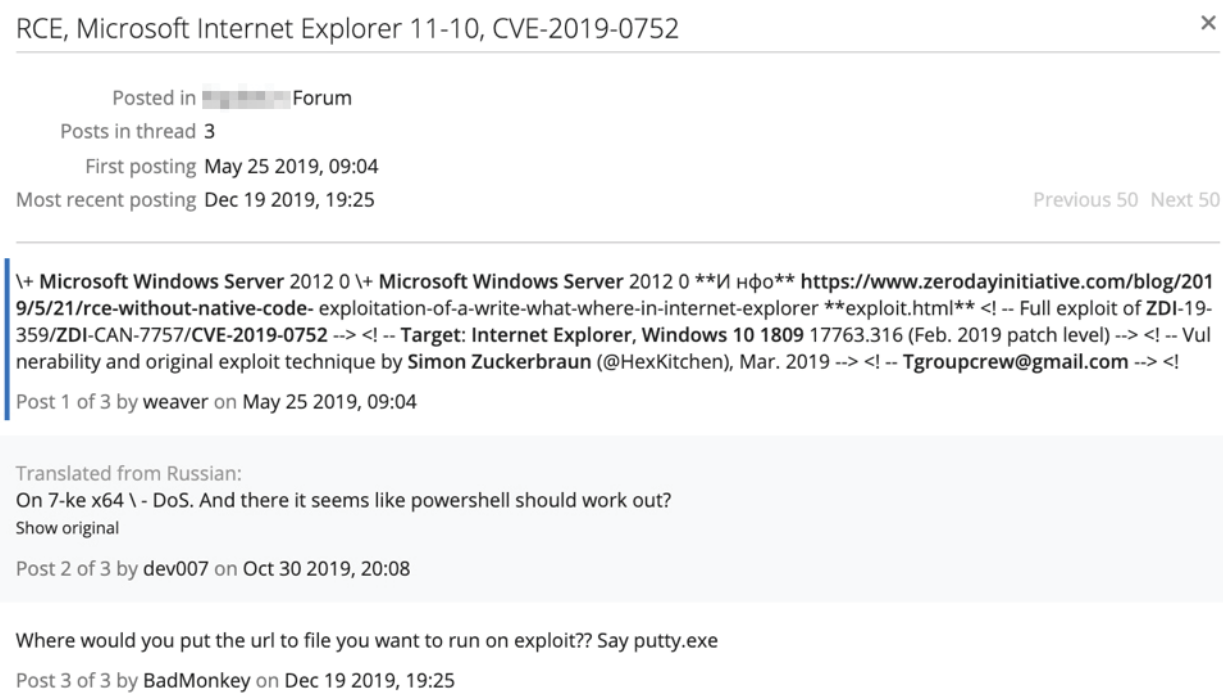
2018년 취약점 1위인 CVE-2018-8174는 2019년 두 번째로 많이 익스플로잇된 취약점이었다. 상위 10위권에 오른 8개의 Microsoft 취약점 중 하나인 CVE-2018-8174("Double Kill")은 Windows VBScripting 엔진에 존재하는 Microsoft Internet Explorer 취약점이다. 원격 코드 실행 취약점인 CVE-2018-8174는 RIG Exploit Kit, Fallout, Spelevo, Capesand에서 사용된다.

위의 두 CVE 모두 2019년에 만들어진 새로운 익스플로잇 키트인 Spelevo와 관련이 있다. Spelevo는 감염된 웹사이트를 통해 패치되지 않은 Internet Explorer와 Adobe Flash 취약점을 공략하고 Maze 랜섬웨어, IcedID, Dridex 멀웨어를 배포한다. 레코디드 퓨처가 2019년 3월 11일에 Pastebin 게시물에서 처음 확인하였으며, 2019년 중반에 이 익스플로잇 키트에 대한 더 많은 분석과 다크웹 토론이 나왔다. 다크웹 소스를 검색하면 Spelevo에 대한 미미한 논의가 있지만 현재 이 익스플로잇 킷이 다크웹 시장에서 공개적으로 판매되고 있음을 나타내는 정보는 없다.

2019년에 발표된 주요 CVE

2019년 가장 많이 익스플로잇된 10대 취약점 목록에서 2019년에 나온 것은 CVE-2019-0752 단 하나 뿐이다. 2018년과 2017년 연례 취약점 보고서에서는 그 해 나온 CVE가 각각 3개씩 포함되어 있었다.

2019년 4월에 패치된 CVE-2019-0752는 Internet Explorer 10과 11에 영향을 주는 "Scripting Engine Memory Corruption Vulnerability"이다. 이 취약점은 Capesand 익스플로잇 키트에 결합되어 있으며, 아래에서 자세히 설명할 것이다. 보안 연구원인 Simon Zuckerbraun이 2019년 5월 CVE-2019-0752에 대해 최초로 자세한 개념 증명(proof of concept)을 하여 Exploit.in과 XSS 같은 언더그라운드 포럼에 배포하였다.


RCE, Microsoft Internet Explorer 11-10, CVE-2019-0752

Posted in [redacted] Forum
Posts in thread 3
First posting May 25 2019, 09:04
Most recent posting Dec 19 2019, 19:25
Previous 50 Next 50

\+ **Microsoft Windows Server** 2012 0 \+ **Microsoft Windows Server** 2012 0 **И нфо** **https://www.zerodayinitiative.com/blog/2019/5/21/rce-without-native-code-** exploitation-of-a-write-what-where-in-internet-explorer **exploit.html** <! -- Full exploit of **ZDI**-19-359/**ZDI**-CAN-7757/**CVE-2019-0752** --> <! -- **Target**: **Internet Explorer**, **Windows 10 1809** 17763.316 (Feb. 2019 patch level) --> <! -- Vulnerability and original exploit technique by **Simon Zuckerbraun** (@HexKitchen), Mar. 2019 --> <! -- **Tgroupcrew@gmail.com** --> <!

Post 1 of 3 by **weaver** on **May 25 2019, 09:04**

Translated from Russian:
On 7-ke x64 \ - DoS. And there it seems like powershell should work out?
Show original

Post 2 of 3 by **dev007** on **Oct 30 2019, 20:08**

Where would you put the url to file you want to run on exploit?? Say putty.exe

Post 3 of 3 by **BadMonkey** on **Dec 19 2019, 19:25**

다크웹 포럼 멤버가 공개한 CVE-2019-0752 익스플로잇.

CVE-2019-0752는 지하 범죄 커뮤니티 외에 2019년 7월 워터링홀(watering hole) 공격에 사용된 SLUB 멀웨어에도 관련되었다. SLUB은 3월에 처음 관찰되었는데, 그 때는 또 다른 2019년 10대 취약점인 CVE-2018-8174를 익스플로잇했다. Trend Micro의 연구원들은 이 워터링홀 공격에 사용된 웹사이트가 북한 관련 사이트라고 보고했다.

2019년에 나온 취약점 가운데 상위 10위권에 포함된 것은 하나 뿐이지만, 20위권까지 넓혀 보면 CVE-2019-0841와 CVE-2019-3396가 순위에 올랐다.

"Sandbox Escaper[2]"라는 닉네임의 사용자가 5월에 공개한 CVE-2019-0841는 Microsoft가 Windows AppX Deployment Service 오류 수정을 위해 발표한 보안 패치를 우회하는 공격을 허용한다. "ByeBear"라는 이름의 익스플로잇은 공격자가 취약점을 이용해 컴퓨터의 제어 권한을 획득하여 악성 코드를 설치하고 데이터를 훔쳐 보거나 파일을 변조 또는 삭제할 수 있게 한다.

[2] Sandbox Escaper는 2018년부터 2019년까지 10개월 동안 8개의 Microsoft 제로데이 취약점을 공개하면서 악명을 얻었다. 익명의 개발자로 알려진 이 인물은 이 취약점들을 Microsoft에 알리지 않고 깃허브에 바로 공개했다고 한다.

2019년 상위 20개 취약점 중 하나인 CVE-2019-3396은 Atlassian Confluence Server 취약점이다. 2019년 4월에 사이버 범죄자들이 Monero를 실행하는 크립토재킹(Cryptojacking) 멀웨어를 설치하는 익스플로잇에서 이 취약점을 처음 이용하였다. 2019년 12월에는 북한 해킹 그룹이 이 취약점을 이용하여 시스템 권한을 탈취하는 DacIs라는 신종 RAT을 배포했다. Windows와 Linux 플랫폼을 공격하는 DacIs는 C2(command and control) 통신 시 TLS와 RC4 암호화를 사용하고, AES 암호화를 사용하여 위장된 구성 파일을 보호한다. 이 취약점에 대한 패치가 나와있다.

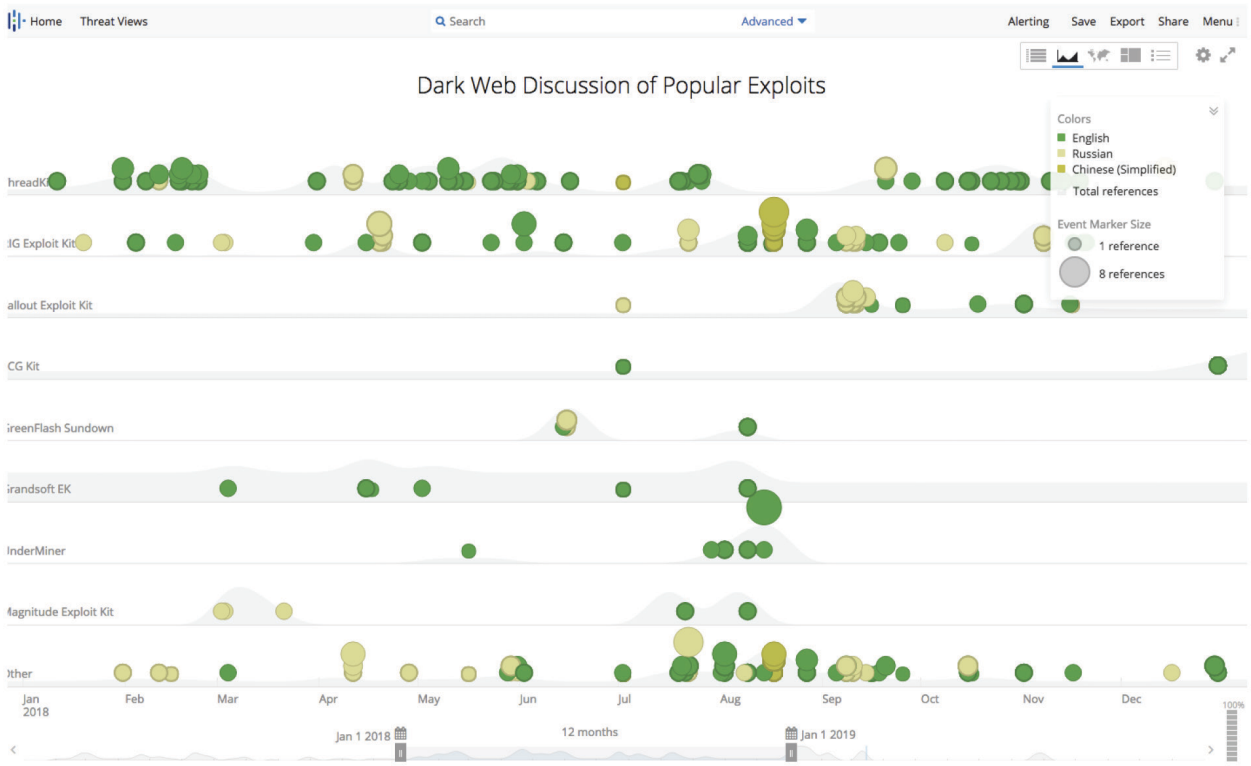
신종 익스플로잇 키트 개발은 감소하는 추세

2019년 들어서 새로운 익스플로잇 키트의 개발은 계속 감소하고 있다. 이는 이전 보고서에서도 확인할 수 있는 추세이다. 2019년에 나온 신종 익스플로잇 키트는 단 4개이다. 2018년 5개, 2017년 10개, 2016년 62개였던 것에 비교하면 확연한 감소 추세이다. 2006년에 등장한 익스플로잇 키트는 전문적인 코딩 능력 없이도 사이버 범죄자가 타겟 시스템에 침투할 수 있게 해줌으로써 범죄 세계에서 가장 인기있는 CaaS(Crimeware as a Service) 중 하나로 각광받았다.

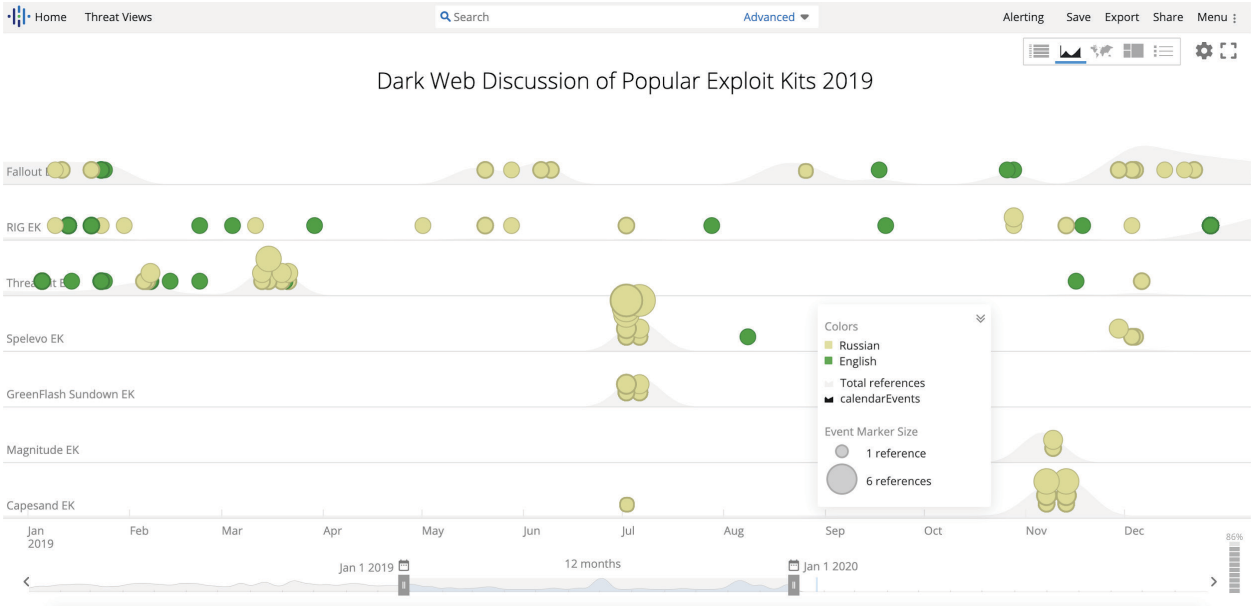
Exploit Kit Name	Technologies Impacted
CapeSand	Microsoft's Internet Explorer (CVE-2015-2419 and CVE-2019-0752); Adobe Flash Player (CVE-2018-4878 and CVE-2018-15982)
Spelevo	Adobe Flash Player (CVE-2018-15928 and CVE-2018-4878); Microsoft's Internet Explorer (CVE-2018-8174)
Lord Exploit Kit	Adobe Flash Player (CVE-2018-15928)
10KBlaze	SAP NetWeaver

2019년 신종 익스플로잇 키트와 영향 받는 기술

2018년에 비해 다크웹에서 익스플로잇 키트에 대한 게시글이 전반적으로 크게 줄어들었다. 가장 인기있는 익스플로잇 키트인 Fallout과 RIG에서도 이런 감소세가 반영된다. 2019년 3월에 처음 나온 신종 익스플로잇 키트 Spelevo는 7월에 반짝 화제가 되었고, 마찬가지로 Capesand도 2019년 연말 즈음에 잠시 게시글이 증가했다.



2018년 주요 취약점 익스플로잇 키트에 대한 다크웹 게시글



2019년 주요 취약점 익스플로잇 키트에 대한 다크웹 게시글

2019년 들어 감소하는 추세이며 해묵은 취약점과 웹 브라우저를 공략함에도 불구하고 익스플로잇 키트 사용이 계속되는 것은 운영자(공격자)가 여전히 트래픽 리디렉션을 통해 수익을 창출할 수 있음을 나타낸다. 레코디드 퓨처의 평가에 따르면 이것은 익스플로잇 키트 서비스에 돈을 지불하는 멀웨어 제작자 덕분이다. 그렇지 않고 익스플로잇 키트 자체로 브라우저를 감염시키는 것만으로는 수익을 창출하기 어렵다. Edge, Chrome, Firefox와 같은 최신 웹 브라우저를 사용함으로써 익스플로잇 키트로 인한 위협을 완화시킬 수 있다. Internet Explorer에는 이러한 익스플로잇 키트에 악용되는 많은 취약점이 존재한다.

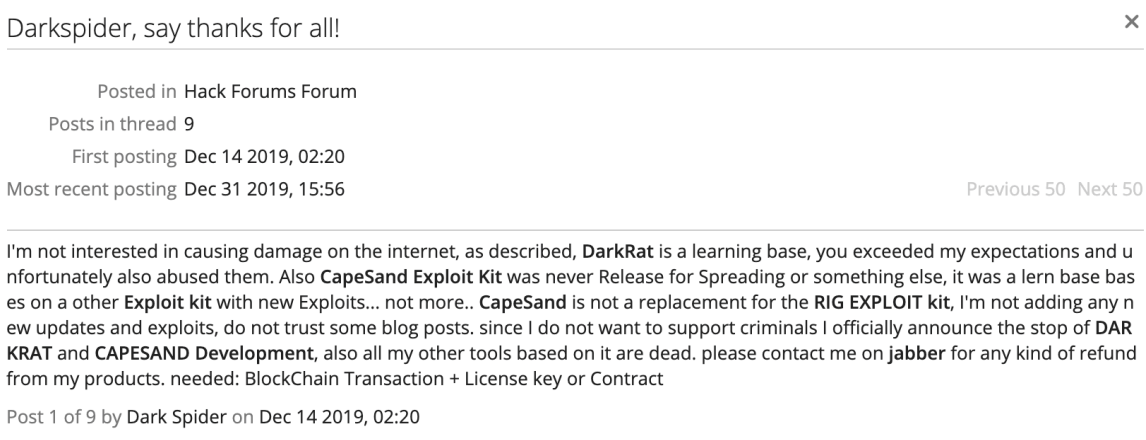
Capesand 익스플로잇 키트

2019년 가장 많이 익스플로잇된 취약점들과 관련된 신종 익스플로잇 키트 중 하나가 Capesand이다. Capesand는 가장 많이 익스플로잇된 10개 익스플로잇 중 4개를 공략한다. Microsoft Internet Explorer의 CVE-2015-2419, CVE-2019- 0752와 Adobe Flash Player의 CVE-2018-4878, CVE- 2018-15982가 바로 그것이다.

TrendMicro의 연구원들이 RIG 익스플로잇 키트를 사용한 멀버타이징(Malvertising) 캠페인을 분석하던 중에 이 신종 익스플로잇 키트를 발견했다. Capesand는 거의 모든 기능이 오픈소스 코드를 기반으로 한다는 점에서 독특하다. 연구원들은 프론트엔드 소스 코드 확인 결과 Capesand가 오래 전 인기를 끌었던 Demon Hunter 익스플로잇 코드와 매우 유사하다는 것을 확인했다. (Demon Hunter는 2008년, 2010년, 2013년 Java, Microsoft, Adobe에 영향을 미치는 다양한 취약점을 노렸음.)

이전 보고서에서는 Capesand를 처음 제작하고 배포한 사용자를 특정하지 못했다. 언더그라운드 포럼의 Capesand 관련 검색 결과, "Dark Spider"라는 사용자가 2019년 12월 중순에 Capesand와 DarkRat의 개발을 중단할 것이라고 주장했다. Dark Spider는 아마도 독일어 사용자이며, 주로 Hack Forums에서 활동하는 것으로 보인다.

Dark Spider는 Capesand와 DarkRat 익스플로잇 키트가 원래 출시용이 아니었으며, 특히 Capesand는 RIG 익스플로잇 키트를 대체하기 위한 것이 아니라고 주장했다. Dark Spider는 Jabber 요청을 통해 환불이 가능하다고 말했다.



Darkspider, say thanks for all!

Posted in Hack Forums Forum
Posts in thread 9
First posting Dec 14 2019, 02:20
Most recent posting Dec 31 2019, 15:56

Previous 50 Next 50

I'm not interested in causing damage on the internet, as described, **DarkRat** is a learning base, you exceeded my expectations and u nfortunately also abused them. Also **CapeSand Exploit Kit** was never Release for Spreading or something else, it was a lern base bas es on a other **Exploit kit** with new Exploits... not more.. **CapeSand** is not a replacement for the **RIG EXPLOIT kit**, I'm not adding any n ew updates and exploits, do not trust some blog posts. since I do not want to support criminals I officially announce the stop of **DAR KRAT** and **CAPESAND Development**, also all my other tools based on it are dead. please contact me on **jabber** for any kind of refund from my products. needed: BlockChain Transaction + License key or Contract

Post 1 of 9 by Dark Spider on Dec 14 2019, 02:20

Hack Forums에 게시된 스레드에서 사용자 Dark Spider가 Capesand 개발을 중단한다고 주장.

2019년 신종 RAT

DacIs는 2019년에 새롭게 등장한 23종의 RAT 중 하나이다. 가장 많이 익스플로잇된 상위 10개 취약점과는 관련이 없으나, 앞서 언급했듯이 20위권 취약점 중 하나인 CVE-2019-3396과 관련 있다

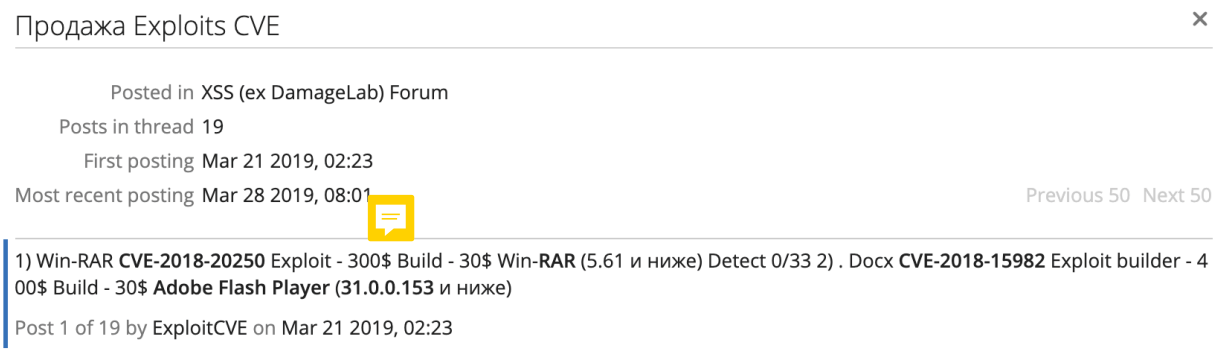
RATs	Cyber Vulnerability Count
QuasarRAT	2
BalkanRAT	1
njRAT	1
RevengeRAT	1
REMCOS RAT	1

가장 많이 익스플로잇된 10개 취약점과 관련된 RAT

2019년 가장 많이 익스플로잇된 취약점과 관련이 있는 신종 RAT는 BalkanRAT 하나이다. BalkanRAT은 Microsoft WinRAR ACE 취약점인 CVE-2018-20250을 노린다. BalkanRAT은 변종 멀웨어인 BalkanDoor와 함께 크로아티아, 보스니아 헤르체고비나, 세르비아, 몬테네그로 등 발칸 지역 기업과 기관을 겨냥한 공격에 사용되었다.

BalkanRAT은 공격자가 그래픽 인터페이스를 통해 감염된 컴퓨터를 원격으로 제어할 수 있도록 해준다. BalkanRAT의 목적은 피해자의 컴퓨터에 Remote Utility 소프트웨어 카피를 설치하는 것이다. BalkanRAT은 정부 웹사이트와 이메일을 모방한 가짜 이메일에 담긴 악성 링크를 통해 배포된다.

2019년 3월에는 언더그라운드 포럼 XSS에 "ExploitCVE"라는 사용자가 CVE-2018-20250에 대한 익스플로잇을 판매한다고 나타났다. 이 위협 행위자의 CVE-2018-20250 익스플로잇 가격은 싱글 빌드 30 달러 또는 모든 WinRAR 5.61 이하 버전에 대해 400 달러였다.



Продажа Exploits CVE

Posted in XSS (ex DamageLab) Forum
Posts in thread 19
First posting Mar 21 2019, 02:23
Most recent posting Mar 28 2019, 08:01

Previous 50 Next 50

1) Win-RAR **CVE-2018-20250** Exploit - 300$ Build - 30$ Win-**RAR** (5.61 и ниже) Detect 0/33 2) . Docx **CVE-2018-15982** Exploit builder - 400$ Build - 30$ **Adobe Flash Player** (**31.0.0.153** и ниже)

Post 1 of 19 by ExploitCVE on Mar 21 2019, 02:23

ExploitCVE가 2019년 3월에 올린 CVE-2018-20250과 CVE-2018-15982에 대한 익스플로잇 판매 게시글.

취약점 별 패치

아래 표는 이 보고서에 나온 가장 많이 익스플로잇된 10개 취약점에 대한 치료 소스 링크를 제공한다.

CVE	치료	레코디드 퓨처 위험 점수
CVE-2018-15982	Adobe는 Flash Player 32.0.0.101 이상에서 이 취약점을 해결했다.	99
CVE-2018-8174 (Double Kill)	Microsoft는 2018년 5월 보안 업데이트에서 이 취약점을 해결했다.	99
CVE-2017-11882	Microsoft는 2017년 11월 29일 Microsoft Office 2007 해당 에디션에 대한 보안 업데이트 4011604와 Microsoft Office 2010 해당 에디션에 대한 보안 업데이트 4011618을 발표했다. Microsoft는 해당 버전의 Office 사용 고객에게 이 취약점 보호를 위한 업데이트 설치를 권고한다. 이전에 릴리스된 업데이트(4011276 또는 2553204)를 이미 설치한 고객은 추가 조치가 필요 없다.	99
CVE-2018-4878	Adobe는 2018년 2월 6일에 릴리스된 버전 28.0.0.161에서 이 취약점을 해결했다.	99
CVE-2019-0752	Microsoft는 2019년 4월 보안 업데이트에서 이 취약점을 해결했다.	89
CVE-2017-0199	Microsoft는 2017년 4월 보안 업데이트에서 이 취약점을 해결했다.	99
CVE-2015-2419	Microsoft는 2015년 7월 보안 업데이트 (MS15-065)에서 이 취약점을 해결했다.	99
CVE-2018-20250	이것은 19년 된 취약점이다. WinRAR은 WinRAR 5.70 Beta 1에서 압축 해제 ACE 아카이브에 대한 지원을 중단하기로 결정했다. 현재 베타 버전은 5.70 Beta 2이다. WinRAR 사용자는 최대한 빨리 최신 베타 버전으로 업그레이드해야 한다.	99
CVE-2017-8750	Microsoft는 2017년 9월 보안 업데이트에서 이 취약점을 해결했다.	89
CVE-2012-0158	Microsoft는 2012년 4월 보안 업데이트 (MS12-027)에서 이 취약점을 해결했다.	99

2019년 주요 취약점에 대한 치료 링크

권장 조치

레코디드 퓨처 연례 취약점 목록의 목표는 다크웹에서 활동하는 사이버 범죄자들이 가장 많이 악용하는 취약점 익스플로잇에 대한 정보를 제공하는 것이다. 보안팀은 이 보고서에 나온 데이터와 다음의 권장 사항을 참고하여 필요한 대응 조치를 취할 수 있다.

- 이 보고서 취약점 목록에 포함된 익스플로잇 수가 너무 많다면 조직의 기술 스택에서 Microsoft 제품 패치를 우선적으로 수행할 것.
- 브라우저 설정에서 Flash Player가 비활성화되어 있는지 확인할 것. (Adobe는 2020년 12월 31일 Flash Player에 대한 지원을 종료할 예정이며 많은 사이트가 이 기술을 제거하고 있음.)
- 이 보고서에 나온 모든 취약점에 대한 패치를 우선적으로 수행할 것.
- 오래된 취약점에 대한 패치를 잊지 말 것. 2017 RAND 보고서에 따르면 평균적으로 취약점은 거의 7년 동안 지속된다.
- 주요 비즈니스 프로세스에 영향을 미치지 않는다면 취약점의 영향을 받는 소프트웨어를 제거할 것.
- 멀버타이징(Malvertising)을 통한 익스플로잇 방지를 위해 브라우저 Ad Blocker를 설치할 것.
- 자주 시스템을 백업할 것. 특히 랜섬웨어 대상이 되는 시스템, 공유 파일이 있는 시스템을 자주 백업할 것.
- 피싱 보안에 대한 인식을 강화할 것. 추가 정보를 요청하거나 링크 또는 첨부 파일을 클릭하도록 유도하는 이메일에 의구심을 갖게 하는 사용자 교육 실시. 기업은 일반적으로 고객에게 개인 정보는 금융 정보를 요구하지 않으며, 의심이 갈 경우에는 전화로 직접 회사에 연락하여 실제로 해당 정보가 필요한지 확인해야 함.
- 취약점 관리팀은 레코디드 퓨처의 기술 정보를 사용하여 멀웨어에 의해 가장 많이 익스플로잇되는 취약점이 무엇인지에 따라 패치 우선순위를 정할 수 있음.

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 특허 받은 머신러닝을 기반으로 한 업계 유일의 완전한 보안 인텔리전스 솔루션을 통해 조직이 위험을 줄일 수 있도록 해줍니다. 레코디드 퓨처의 기술은 타의 추종을 불허하는 방대한 소스로부터 자동으로 정보를 수집하고 분석합니다. 그리고 사람의 분석 또는 기존 보안 기술과의 통합을 위한 귀중한 컨텍스트를 실시간으로 제공합니다.