FIREEYE iSIGHT INTELLIGENCE

폭풍의 중심에서

러시아 해킹 그룹 APT28, 사이버 공격을 전략적으로 진화시키다

SPECIAL REPORT / JANUARY 2017

FireEye

CONTENTS

개요 3

개관 4

APT28 타깃 설정과 침투 활동 5

표 1 – APT28의 정치조직 타깃 설정 및 침투 활동 6

표 2 - APT28의 네트워크 활동이 여러 정보 작전을 지원했을 가능성이 있음 7

올림픽 망신부터 데이터 유출까지 : APT28의 세계반도핑기구 공격에 대한 조사 8

결론 10

APT28 악성코드 및 전술 11

개요

2016년 6월, 미국 민주당전국위원회(DNC)는 DNC 네트워크 침해 사건의 범인을 러시아 정부로 지목했고, 이로 인해 대미 정보 작전에 대한 러시아 정부의 지원을 둘러싸고 국제적인 논란이 벌어졌다.

러시아 정부가 해킹 사건 및 관련 데이터 유출에 책임이 있는 해킹 그룹에 직접 지시를 내렸는지, 만약 그랬다면 그것이 용인될 수 있는 국가 첩보 활동인지 아니면 선을 넘은 행위인지, 또 DNC 침해가 미국 대선에 개입하고자 하는 러시아 정부의 더 광범위한 노력의 일부인지 등에 대한 증거의 문제가 현재 쟁점이 되고 있다.

미국 정부, 보안 업체 및 피해 조직들은 이에 대한 답을 찾기 위해 2016년 침해사건을 저지른 공격자들을 식별할 수 있는 정보, 특히 우리가 APT 28이라고 부르는 그룹에 대한 정보를 제출했다. 그 후 2016년 12월 29일, 미 국토안보부와 FBI는 FireEye가 오랫동안 견지해온 평가 즉, 러시아 정부가 APT28의 스폰서라는 내용을 확인해주는 공동 분석 보고서를 발표했다. FireEye는 수많은 조사, 엔드포인트 및 네트워크 탐지 및 지속적인 모니터링을 통해 이 그룹을 추적 및 프로파일링 해왔으며, 이를 통해 APT28이 사용하는 악성코드, 작전 상의 변화 및 동기를 이해할 수 있었다. 이 인텔리전스는 FireEye 고객을 보호하고, 고객에게 공격에 관련된 정보를 제공하며, 이 공격을 노출시키는 데 중요한 역할을 하였다.

개관

적어도 2007년 이래로, APT28은 러시아의 전략적 이익을 지원하는 광범위한 작전에 참여해왔다. 고도화된 능력으로 수많은 공격을 수행할 수 있는 개발자와 공격자를 가진 이 그룹은 계속해서 국방 및 지정학적인 문제에 대한 인텔리전스를 수집해왔다. APT28 의 첩보 활동은 정부, 군, 대사관의 국방 담당관, 미디어 조직, 반체제 인사 및 현 러시아 정부에 반대하는 인물 등을 포함해, 주로 미국, 유럽, 전 소련 소속 국가의 조직들을 타깃으로 삼았다.

지난 2년 간 러시아는 자국 군의 광범위한 전략적 원칙에 맞는 정보전을 수행하는데 있어 APT28을 점점 더 많이 활용해왔다. APT28은 피해 조직을 침해한 후, 러시아에 이익이 되는 정치적 내러티브를 전개하는 데 이용할 수 있는 내부 데이터를 유출, 공개해왔다. 이런 사례에는 시리아 갈등 사태, NATO-우크라이나 관계, EU 난민 및 이민 위기, 2016년 올림픽 및 패럴림픽 러시아 팀 도핑 스캔들, 러시아 정부가 지원하는 해킹에 대한 공개적인 비난, 2016년 미국 대선 등이 모두 포함된다.

본 보고서는 APT28의 타깃 설정에 대한 관찰 결과 및 관련 침해 사고, 툴 개발 및 이용 상의 변화, 피해자를 침해하기 위한 APT28의 전술 등에 대한 조사를 상세히 담고 있다.

APT28 타깃 설정과 침투 활동

2014년 10월, FireEye는 보고서 APT28: A Window into Russia's Cyber Espionage Operations?(APT28: 러시아의 사이버 첩보 활동의 창구인가?)를 발표하며 APT28 활동의 성격이 러시아 정부의 전략적 정보 요구사항과 일치한다고 밝혔다. APT28을 추적하는 동안 우리는 이 그룹이 외국 정부와 군, 특히 유럽과 동유럽 국가들의 정부 및 군에 관심이 있다는 사실을 알아냈고, 또한 여러 조직 중에서도 NATO(북대서양조약기구), OSCE(유럽안보협력기구) 등 지역 안보 조직에 관심이 높다는 사실을 알 수 있었다.

표 1: APT28의 정치조직 타깃 설정 및 침투 활동

조직	시기	APT 타깃 설정 및 침투 활동
유럽안보협력기구(OSCE)	2016년 11월	OSCE는 침해가 있었다는 사실을 인정했고, 서방의 한 정보 기관은 이 공격의 공격자로 APT28를 지목했다.[1]
독일 기독교 민주 동맹(CDU)	2016년 4-5월	Trend Micro의 연구자들은 APT28이 CDU 당원들의 이메일 인증정보를 알아내어 그들의 계정에 접근하기 위해 가짜 CDU-이메일 서버를 만들어 CDU 당원들에게 피싱 이메일을 보냈다는 사실을 확인할 수 있었다.[2,3]
푸시 라이엇(Pussy Riot)	2015년 8월	APT28이 반체제 성향의 러시아 락 밴드 푸시 라이엇를 대상으로 스피어 피싱 이메일 공격을 수행하였다.[4]
NATO, 아프가니스탄 외교부, 파키스탄 군	2015년 7월	APT28은 Adobe Flash 제로데이 익스플로잇을 호스팅하기 위해 2개의 도메인을 사용하여 (nato-news.com, bbc-news.org) NATO, 아프가니스탄 외교부, 파키스탄 군을 타깃 공격하였다.
독일 하원 및 정당	2015년 6월	독일 BSI(Federal Office for Security in Information Technology)는 APT28이 몇몇 독일 정당의 당원에게 전송된 피싱 이메일의 범인일 가능성이 높다고 발표했다. 독일 국내 정보 조직인 BfV(Bundesamt für Verfassungsschutz)의 수장 역시 2015년 독일 하원 네트워크 침해의 범인으로 APT28를 지목했다.[5,6]
키르기스스탄 외교부	2014년 10월부터 2015년 9월까지	FireEye iSight는 DNS(domain name server) 기록에서 APT28이 키르기스스탄 외교부의 DNS 서버를 악의적으로 변경한 후 외교부의 이메일 트랙픽을 가로챘다는 것을 암시하는 변경 사항들을 발견할 수 있었다.
폴란드 정부 및 Power Exchange 웹사이트	2014년 6월 및 9월	APT28은 전략적 웹 침해와 더불어 "Sedkit"를 이용하여 "Sofacy" 악성코드를 폴란드 정부의 여러 웹사이트와 폴란드 에너지 기업인 Power Exchange의 웹사이트에 심었다.[7]

1. Gauquelin, Blaise. "La Russie soupçonnée d'être responsable d'un piratage informatique contre l'OSCE." Le Monde. 28 Dec. 2016. Web. 29 Dec. 2016.
2. Trend Micro refers to activity corresponding to FireEye's APT28 as "Pawn Storm."
3. Hacquebord Feike. "Pawn Storm Targets German Christian Democratic Union." Trend Micro. 11 May 2016. Web. 29 Dec. 2016.
4. Hacquebord Feike. "Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets." TrendLabs Security Intelligence Blog, Trend Micro. 18 August 2015. Web. 29 Dec. 2016.
5. "Neuer Hackerangriff auf Bundespolitiker / BSI warnt Parteien vor Cyberangriffen." Westdeutscher Rundfunk. 20 Sept. 2016. Web. 29 Dec. 2016.
6. "Russia 'was Behind German Parliament Hack.'" The BBC. 13 May 2016. Web. 29 Dec. 2016.
7. Kharouni, Loucif. et al. "Operation Pawn Storm: Using Decoys to Evade Detection." Trend Micro. 22 Oct. 2014. Web. 3 Jan. 2017.

2014년 이래로, APT28은 외국의 정치적 상황에 영향을 미치기 위해 설계된 작전도 수행했다. 이러한 작전 중 일부는(아래표 참조) 웹사이트 방해 및 손상, false flag operation, 온라인 상에 공개할 데이터의 유출 등을 포함한다. 겉으로는 달라 보일지라도 이 작전들은 모두 유사한 목표 즉, 러시아에 이로운 정치적 결과를 달성하기 위해 수행된 것들이다.

표 2: APT28 네트워크 활동이 여러 정보작전을 지원했을 가능성이 있음

피해 조직	시기	APT28 네트워크 활동	연관된 정보 작전
세계반도핑기구 (WADA)	2016년 9월	2016년 9월 13일, 세계반도핑기구(WADA)는 APT28이 WASA의 네트워크를 침해했고, 선수들의 의료 데이터에 접근했다고 인정했다.[8]	2016년 9월 12일, "Fancy Bears' Hack Team"의 신원으로 활동하는 공격자가 자신이 WADA를 침해했다고 주장하며 "미국 선수들의 도핑에 대한 증거"로 선수들의 의료 기록을 공개했다.[9]
미국 민주당 전국위원회(DNC)	2016년 4월–9월	미국 민주당 전국위원회(DNC)는 DNC가 네트워크 침해를 겪었으며 이후의 조사에서 APT28과 APT29의 소행으로 생각되는 2건의 침해에 대한 증거를 발견했다고 발표했다. FireEye는 DNC 네트워크에서 발견된 악성코드를 분석하였고, 이 코드가 이전부터 관찰해 온 APT28의 툴과 일치한다고 결론지었다.[10,11]	2016년 6월, DNC의 발표가 있은 지 얼마 후 "Guccifer 2.0" 신원으로 활동하는 공격자가 DNC 침해가 자신의 소행이라고 주장하며 DNC의 네트워크로부터 유출한 문서들을 공개했다. Guccifer 2.0은 9월 동안 계속해서 여러 DNC 문서들을 공개했다.[12,13]
존 포데스타(John Podesta)	2016년 3월–11월	조사자들은 보안 전문가들이 APT28의 소행이라고 판단한 단축 URL을 이용한 대규모 피싱 공격의 타깃이었던 수천 명 중에 힐러리 클린턴 미 대통령 후보의 선거 위원장이었던 존 포데스타가 포함되어 있었다는 사실을 알아냈다.[14]	10월부터 11월 초까지 WikiLeaks는 계속해서 존 포데스타의 개인 이메일 계정에서 유출한 34편의 이메일 통신 내용을 공개했다. 콜린 파웰(Colin Powell) 전 국무부 장관과 클린턴 선거 캠프의 직원이었던 윌리엄 라인하트(William Rinehart) 등 이 동일한 피싱 공격의 타깃이 되었던 다른 개인들의 이메일 통신 내용 또한 "DC Leaks" 웹사이트에 공개되었다.[15]
미국 민주당 하원 선거위원회 (DCCC)	2016년 3월–10월	2016년 7월, 미국 민주당 하원 선거위원회(DCCC)는 DCCC가 FBI가 민주당 전국위원회(DNC) 침해 사건과 관계가 있다고 추정하고 있는 "사이버 보안 사건"을 현재 조사하고 있다고 발표했다. 민주당 하원 원내 대표 낸시 펠로시(Nancy Pelosi)는 후에 DCCC 네트워크에 침해가 있었다고 인정했다. 조사자들은 공격자가 이보다 훨씬 전인 3월부터 DCCC 네트워크에 접근이 가능했을 가능성이 있음을 시사했다.[16,17,18]	2016년 8월, "Guccifer 2.0"이라는 신원으로 활동하는 공격자가 미국의 여러 하원 선거를 다루는 기자들에게 연락을 취해, 민주당 후보들과 연관된 문서들을 새로이 유출했다고 알려왔다. Guccifer 2.0은 8월부터 10월까지 "그의" WordPress 사이트에 DCCC 내부 문서로 보이는 일부 문서를 추가적으로 포스팅했다.[19,20]
TV5Monde	2015년 2월, 4월	2015년 2월, FireEye는 TV5 Monde의 네트워크에서 CORE-SHELL traffic beaconing 활동을 발견했으며, APT28이 TV5의 네트워크를 침해했음을 확인했다.	2015년 4월, 친 ISIS 그룹이라고 여겨지는 CyberCaliphate가 TV5Monde의 웹사이트와 SNS 프로필을 훼손했으며 TV-5Monde 11개 채널의 방송 송출에 장애를 일으켰다. FireEye는 CyberCaliphate 웹사이트의 도메인 등록 세부사항과 APT28의 인프라에 겹치는 부분이 있다는 사실을 알아냈다.[21]
우크라이나 중앙선거관리위원회 (CEC)	2014년 5월	우크라이나 관계자들은 중앙선거관리위원회(CEC)의 내부 네트워크 침해에 대한 조사가 APT28의 것으로 추적 조사된 악성코드를 발견했다고 발표했다.[22]	2014년 5월에 있었던 우크라이나 대선 도중, 친 러시아 핵티비즘 그룹 CyberBerkut라 알려진 공격자가 CEC에 대해 시스템 침해, 데이터 파괴, 데이터 유출, DDoS 공격 및 가짜 선거 결과로 CEC 웹사이트를 훼손하고자 했던 시도를 포함한 일련의 악의적 활동을 수행하였다.[23]

8. "WADA Confirms Attack by Russian Cyber Espionage Group." World Anti-Doping Agency. 13 Sept. 2016. Web. 29 Dec. 2016.
9. Fancy Bears' HT (fancybears). "@AnonPress Greetings. We hacked #WADA. We have Proof of American Athletes taking doping. Fancybear.net." 12 Sept. 2016, 4:12 PM. Tweet.
10. CrowdStrike refers to activity corresponding to FireEye's APT28 and APT29 as "Fancy Bear" and "Cozy Bear," respectively.
11. "Nakashima, Ellen. "Cyber Researchers Confirm Russian Government Hack of Democratic National Committee." The Washington Post. 20 June 2016. Web. 29 Dec. 2016.
12. "Rid, Thomas. "All Signs Point to Russia Being Behind the DNC Hack." Motherboard, Vice. 25 July 2016. Web. 29 Dec. 2016.
13. "Bennett, Cory. "Guccifer 2.0 Drops More DNC Docs." Politico. 13 Sept. 2016. Web. 2 Jan. 2017. <>
14. Perlroth, Nicole. Shear, Michael D. "Private Security Group Says Russia was Behind John Podesta's Email Hack." The New York Times. 21 Oct. 2016. Web. 2 Jan. 2017.
15. "Franceschi-Bicchierai, Lorenzo. "How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts." 20 Oct. 2016. Web. 2 Jan. 2017.
16. "Nakashima, Ellen. "FBI Probes Suspected Breach of Another Democratic Organization by Russian Hackers." The Washington Post. 29 July 2016. Web. 29 Dec. 2016.
17. "Pelosi, Nancy. "DCCC Cyber Breach." 13 August 2016. Email. U.S. House of Representatives. Washington, DC. Politico. Web. 29 Dec. 2016.
18. "Lipton, Eric. Shane, Scott. "Democratic House Candidates Were Also Targets of Russian Hacking." The New York Times. 13 Dec. 2016. Web. 29 Dec. 2016.
19. Ibid.
20. Gallagher, Sean. "Guccifer 2.0 Posts DCCC Docs, Says They're From Clinton Foundation." Ars Technica. 4 Oct. 2016. Web. 3 Jan. 2017.
21. "Russian Hackers Suspected in French TV Cyberattack." Deutsche Welle. 6 Oct. 2015. Web. 29 Dec. 2016.
22. Joselow, Gabe. "Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past." NBC News. 3 Nov. 2016. Web. 29 Dec. 2016.
23. Clayton, Mark. "Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers (+Video)." The Christian Science Monitor. 17 June 2014. Web. 2 Jan. 2017.

올림픽 망신부터 데이터 유출까지:
APT28의 세계반도핑기구 공격에 대한 조사

미국 민주당전국위원회(DNC) 침해 사건에 대한 소식이 퍼지고 있을 무렵, APT28은 또 다른 공격을 준비하고 있었다. 러시아 팀 도핑 스캔들 이후에 러시아가 직면하고 있던 비난 및 다가오는 리우 올림픽에 러시아 선수를 출전 금지시키겠다는 주장에 대해 역공격을 펼치는 것이었다. 다른 여느 국가들처럼 러시아 역시 올림픽 대회에서의 성공이 세계 무대에서 국가의 힘을 보여주는 것이라 생각해왔다. 이 때문에 도핑 스캔들 및 올림픽 출전 금지에 대한 가능성은 러시아를 더욱 배척시켰고, 러시아가 이러한 주장에 대해 적극적으로 대응할 수 있도록 하는 정당한 구실을 만들어 준 것으로 보인다. APT28의 WADA 네트워크 침해 및 관련 사건에 대한 우리의 조사는 러시아가 어떻게 자국에 피해를 주는 내러티브를 반박하고 러시아에 대한 WADA의 비난을 정당하지 못한 것으로 만들려고 했는지 보여준다.

러시아 선수들의 만연한 도핑에 대한 주장

7월 16일

WADA가 의뢰한 보고서에서 러시아 선수들의 만연한 도핑에 대한 증거가 드러남[24]

7월 18일

WADA가 러시아 반도핑기구를 미준수(NON-COMPLIANT) 기구로 지정하고 러시아 팀을 다가오는 올림픽에서 출전 금지시키도록 제안함[25]

8월 4일

IOC가 러시아 올림픽 팀에서 118명의 선수를 제외함[26]

APT28가 세계반도핑기구(WADA)를 침해

8월 4-8일

APT28이 WADA 직원들에게 각종 스피어 피싱 이메일을 보냄[27]

8월 10일

APT28이 율리아 스테파노바(YULIYA STEPANOVA)의 정상 사용자 계정을 이용하여 WADA의 ADAMS (ADMINISTRATION AND MANAGEMENT SYSTEM)에 로그인함. 스테파노바는 러시아 선수들의 만연한 도핑을 폭로한 WADA의 독립위원회의 위원이었음.[28]

8월 25일-9월 12일

APT28은 2016년 올림픽을 위해 특별히 생성된 IOC 계정에 접근해 선수들의 데이터를 열람하고 다운로드함[29]

24. "Russia State-Sponsored Doping Across Majority of Olympic Sports, Claims Report." The BBC. 18 July 2016. Web. 29 Dec. 2016.
25. Ibid.
26. Macguire, Eoghan. Almasy, Steve. "271 Russian Athletes Cleared for Rio Games." CNN. 5 August 2016. Web. 29 Dec. 2016.
27. "Cyber Security Update: WADA's Incident Response." World Anti-Doping Agency. 5 Oct. 2016. Web. 3 Jan. 2017.
28. "WADA Confirms Attack by Russian Cyber Espionage Group." World Anti-Doping Agency. 13 Sept. 2016.
29. "WADA Confirms Another Batch of Athlete Data Leaked by Russian Cyber Hackers 'Fancy Bear.'" World Anti-Doping Agency. 14 Sept. 2016. Web. 29 Dec. 2016. <>

"FANCY BEARS' HACK TEAM"이 WADA 침해 및 선수 데이터 유출이 자신의 소행이라 주장

8월 9일

"Anonymous Poland"를 대변한다는 주장하는 공격자 @anpoland가 자신이 WADA 웹사이트를 공격했다고 주장했다.[30]

8월 11일

8월 11일, @anpoland는 WADA에 DDos 공격을 수행하고 관련 문서를 유출하겠다고 협박했지만, 이 협박을 실제로 완수하지는 못했다.[31,32]

9월 12일

스스로를 "Fancy Bears' Hack Team"이라 부르는 공격자들이 트위터를 통해 자신들이 WADA의 네트워크를 침해했다고 주장하며, 팔로워들을 그들의 웹사이트 fancybears[.]net 으로 이끌었다.[33]

또한 해외 기자들 및 핵티비즘과 정보 보안 뉴스를 배포하는 것으로 알려진 계정들에 보내는 유사한 트위터 글에서 "Fancy Bears"는 "미국 선수들의 도핑에 대한 증거"를 가지고 있다고 주장했다.[34]

9월 13일

WADA는 침해를 인정하는 성명을 발표했고, 침해 사건과 선수들의 의료 데이터 유출의 범인으로 APT28을 지목했다.[35]

SEP 15-30

9월 동안 "Fancy Bears"는 미국 선수들을 포함한 유명 운동선수들의 의료 파일을 공개했는데, 이들은 약물에 대한 치료목적사용면책(TUE: Therapeutic Use Exemptions)을 신청해서 인정받은 선수들로 그렇지 않았으며 대회에서 출전 금지되었을 선수들이었다.[36]

공정한 경쟁과 깨끗한 스포츠를 지지한다고 주장하는 "Fancy Bears"는 TUE를 "도핑 허용 면허"라고 불렀다.[37]

한편 주 영국 러시아 대사관은 트위터에 "Wada 해킹: 매우 공적인 자료인 올림픽 참가자들의 도핑 파일에는 어떠한 사심도 있어서는 안 된다. 어떤 선수는 다른 선수에 비해 더 평등한가?"라고 남겼다.

WADA 관계자들은 사법기관으로부터 제공받은 증거를 들어 해당 공격 활동이 러시아에서 발생한 것이며 아마도 WADA가 정부 지원을 받은 러시아 선수들의 만연한 도핑을 폭로한 것에 대한 보복일 것이라고 주장하는 성명을 발표했다.[38] 러시아 정부는 이 성명의 내용을 즉각 부인했으며, 러시아 체육부 장관인 비탈리 뭇코(Vitaly Mutko)는 "그 해커들이 러시아 출신이라는 것을 어떻게 증명할 것인가? 모든 사건에 대한 책임을 러시아에게 돌리는 것이 유행인 것 같다."라고 말했다.[39]

30. [OP PL]. "www.tas-cas.org." Online video clip. YouTube. YouTube, 9 Aug. 2016. Web. 3 Jan. 2017.
31. Anonymous Poland (@anpoland). "@Cryptomeorg @ben_rumsby @PogoWasRight @Jason_A_Murdock @Cyber_War_News @kevincollier Tomorrow will ddos WADA and publish some secret dosc." 11 Aug 2016 10:10 AM. Tweet.
32. Anonymous Poland (@anpoland). "@JoeUchill within a few days will be new attack on the WADA/Olimpic." 5 Sept. 2016 5:19 AM. Tweet.
33. Fancy Bears' HT (fancybears). "@AnonPress Greetings. We hacked #WADA. We have Proof of American Athletes taking doping. Fancybear.net."
34. Ibid.
35. "WADA Confirms Attack by Russian Cyber Espionage Group."World Anti-Doping Agency.13 Sept. 2016.
36. Russian Hackers Leak Simone Biles and Serena Williams Files." The BBC. 13 Sept. 2016. Web. 29 Dec. 2016.
37. Rumsby, Ben. "US Superstars Serena and Venus Williams and Simone Biles Given Drugs Exemption, Russian Hackers Reveal." The Telegraph. 14 Sept. 2016. Web. 29 Dec. 2016.
38. Luhn, Alec."Fancy Bears Origins Unclear But Russia Seizes Chance to Put Boot into Wada." 15 Sept. 2016. Web. 29 Dec. 2016.
39. Gibson, Owen. "Russian Sports Minister Vitaly Mutko Denies Link to Wada Hackers." The Guardian. 14 Sept. 2016. Web. 29 Dec. 2016.

결론

2014년 보고서를 발표한 이래로 FireEye는 계속해서 APT28이 러시아 정부의 후원을 받고 있다고 평가해왔다. 에에 더해 우리는 APT28이 WADA, DNC 및 2016년 미 대선과 연관된 여러 조직에 대한 네트워크 침해를 수행했다고 평가한다. 이 침해 사건들은 후에 다양한 포럼에 전략적으로 유출되어 러시아 정부의 특정 목표를 진척시키기 위한 의도라는 것이 거의 확실한 철저히 계산된 방식으로 선전 유포된 내부 데이터(대부분 이메일) 유출과 관련되어 있다. 2017년 1월 7일 발표된 보고서에서 미 국가정보국은 이러한 활동을 "영향력 행사 공격"이라 묘사했다.

네트워크 침해와 후속 데이터 유출이 결합된 영향력 행사 공격은 러시아 군이 공개적으로 밝힌 의도 및 러시아 군이 보유한 역량에 매우 부합하는 공격이다. "정보 작전"이라고도 불리는 영향력 행사 작전은 오래 동안 러시아의 전략적 원칙에 포함되어 왔고, 의도적으로 개발, 사용되어 왔으며 인터넷의 출현과 함께 현대화되었다. 미국에서 발생한 최근의 활동은 러시아 정부가 전략적인 정치 목표 달성을 위해 수행해 온 수많은 공격 중 하나의 사례일 뿐으로, 이 공격이 결코 마지막이지는 않을 것이다. 독일, 프랑스, 네덜란드 등 유럽 국가들의 2017년 선거에 다가옴에 따라, FireEye 벌써부터 이와 유사한 노력의 조짐을 목격하고 있다.

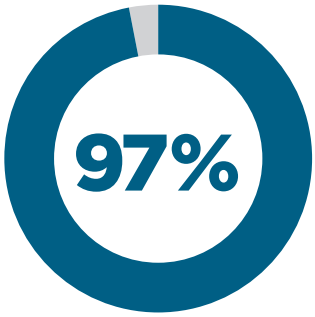
APT28 악성코드 및 전술

APT28이 네트워크 공격을 수행하기 위해 사용하는 툴을 살펴보면 이 그룹이 러시아 정부의 지원을 받으며 활동하고 있다는 주장의 증거가 된다. APT28가 사용하는 일련의 악성코드들은 지속적인 작전 수행에 대한 APT28의 계획 및 여러 자원과 유능한 개발자에 대한 그들의 높은 접근성을 보여준다.

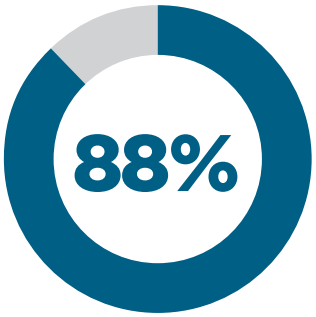
APT28 툴셋의 주요 특징은 다음과 같다:

- APT28이 지속적으로 툴셋을 진화시켜 향후 공격에 계속 사용할 수 있도록 해주는 **융통성 있는 모듈식의 구조**
- 자신의 백도어 내의 다양한 모듈을 추적하고 정의할 수 있도록 **공식적인 코딩 환경** 내에서 툴을 개발
- 분석 환경을 확인하기 위한 실행 시간 체크, 실행 시간에 나타나는 난독화된 문자열들, 분석 속도를 늦추기 위해 사용하지 않는 기계 명령어의 포함 등 **역분석(counter-analysis) 역량을 포함**
- **모스크바 표준시간대의 정상 근무 시간에 러시아 언어 기반 환경에서 컴파일된 코드**

OVER



APT28의 악성코드 샘플 중 97% 이상이 평일에 컴파일링되었으며



88%는 모스크바와 생피터스버그 등 주요 러시아 도시를 포함하는 UTC +4 시간대의 오전 8시에서 오후 6시 사이에 컴파일링되었다.

또한, APT28의 개발자들은 2013년까지 지속적으로 러시아 언어 세팅에서 악성코드를 개발했다.

2013

APT28의 악성코드 세트

TOOL	ROLE	AKA
CHOPSTICK	backdoor	Xagent, webhp, SPLM, (.v2 fysbis)
EVILTOSS	backdoor	Sedreco, AZZY, Xagent, ADVSTORESHELL, NETUI
GAMEFISH	backdoor	Sednit, Seduploader, JHUHUGIT, Sofacy
SOURFACE	downloader	CORESHELL, Sofacy의 구 버전
OLDBAIT	credential harvester	Sasfis
CORESHELL	downloader	SOURFACE, Sofacy의 신 버전

2014년 이후 APT28 작전 상의 변화

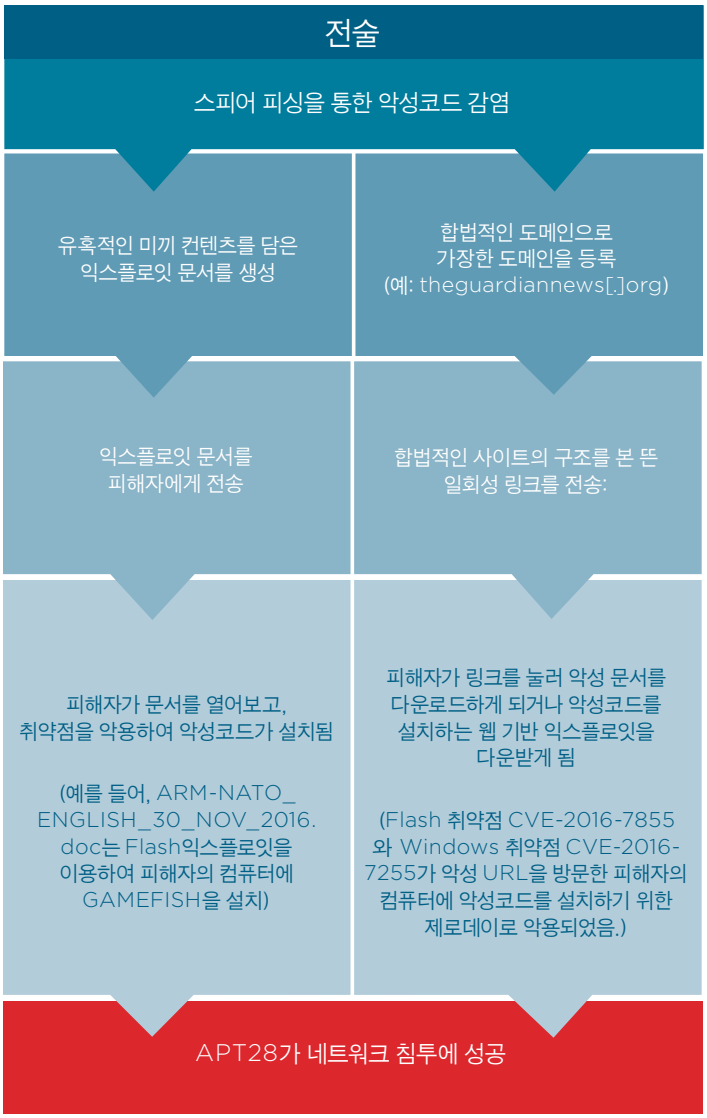
APT28은 계속해서 툴킷을 진화시키고 전술을 다듬어나가고 있는데, 이는 거의 확실히 증가된 대중 노출과 감시 속에서 그들이 수행하는 작전의 효과를 지키기 위한 노력으로 보인다. 이 그룹의 1단계 툴의 진화에 더해, 우리는 또한 APT28의 작전에서 아래의 변화를 목격했다:

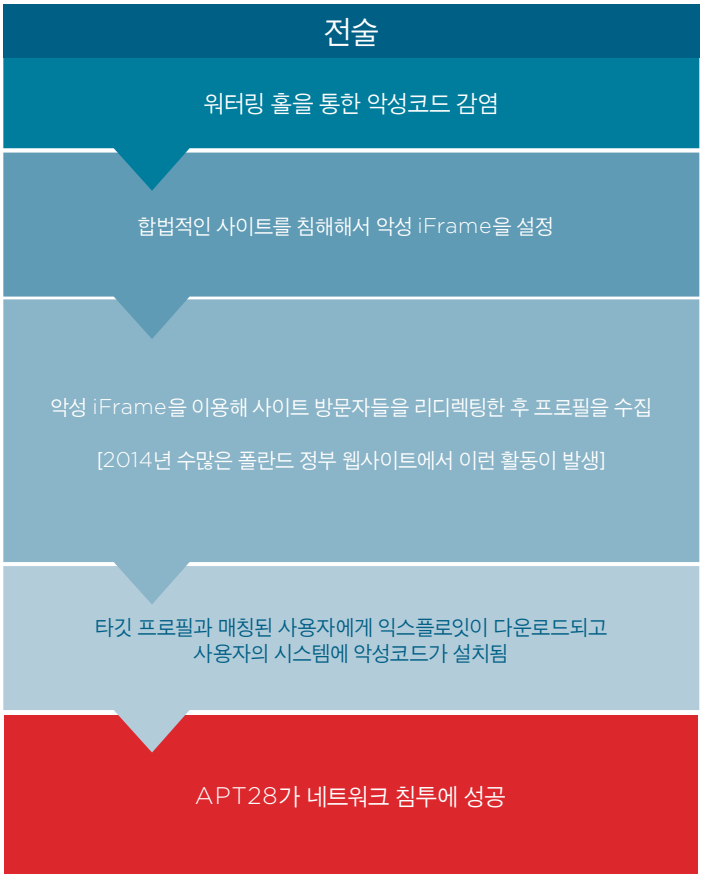
- CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2015-5119, and CVE-2015-7645를 포함해 Adobe Flash Player, Java, Windows 시스템의 **제로데이 취약점을 이용**
- 제로데이 및 다른 툴들을 더욱 선별적으로 사용하기 위해 조사자나 다른 주체가 APT28 툴에 접근할 수 있는 가능성을 감소시키는 **프로파일링 스크립트를 이용**
- 개발 사이클을 가속화하고 공격자를 알아내는 것을 어렵게 만들기 위해 Carberp, PowerShell Empire, P.A.S. webshell, Metasploit 모듈 등 **공개 코드 저장소에 대한 의존도를 높임**
- APT28이 이중 인증과 기타 보안 조치들을 우회하도록 도와주는 **위조된 Google App 인증과 Oauth 접근 요청 을 통해 인증 정보를 획득**
- 침해 기간의 연장을 위해 때로 기존에 사용하던 자신의 툴을 포기하면서까지 피해 시스템에 이미 존재하는 **합법적인 툴만을 사용해 네트워크 내부를 이동**

이러한 변화들은 APT28의 능력, 지략 및 작전의 효과를 유지하고자 하는 그들의 바람을 나타내줄 뿐 아니라 이 그룹의 미션과 가까운 미래에 활동을 지속하고자 하는 APT28의 의도가 장기적인 것이라는 점을 잘 보여준다.

APT28 전술

우리는 APT28이 공격하고자 하는 타깃을 침해할 때 4가지 주요 전술에 의존하는 것을 볼 수 있었다. 이는 사용자의 시스템에 악성코드를 심는 익스플로잇 문서 또는 피해자의 계정에 접근하기 위해 수신자의 이메일 인증정보를 수집하도록 설계된 악성 URL을 포함한 스피어 피싱 이메일을 보내는 활동을 포함한다. APT28은 또한 방문자를 감염시키고자 하는 의도로 합법적인 웹사이트를 침해하여 악성코드를 심어놓기도 하였으며, 웹 페이싱 서버(web-facing server)를 침해함으로써 타깃 조직에 대한 접근을 확보하기도 했다.





To download this or other
FireEye iSIGHT Intelligence reports,
visit: **www.fireeye.com/reports.html**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워20층 02.2092.6580 / korea.
info@fireeye.com

www.FireEye.kr

© 2016 FireEye, Inc. 저작권 소유. FireEye는 FireEye, Inc의 등록상표입니다. 다른 모든 브랜드,
제품 또는 서비스 명칭은 각 소유자의 상표 또는 서비스 마크입니다. WP.FES.EN-US.082016