**FireEye, SolarWinds Hacks Show that Detection is Key to Solid Defense**

By: Anomali Threat Research December 17, 2020

카테고리: [**MALWARE**](https://www.anomali.com/blog/category/malware)**,**[**RESEARCH**](https://www.anomali.com/blog/category/research)​

몇 년 전, 업계 분석 회사인 Gartner는 거의 모든 주요 기업과 정부 기관의 시스템이 해커에 의해 어느 시점에는 손상되거나 손상될 것이라고 했습니다. 이번 주에 FireEye와 SolarWinds가 해킹을 당했다는 소식을 듣고 Gartner가 옳았다는 사실을 다시 한 번 알게 되었습니다. 고급 보안 전문 지식과 방대한 리소스를 보유한 기업조차도 디지털 생활에서의 불가피한 사실에서 벗어날 수 없습니다.

포렌식 전문가와 언론 기관은 이제 디지털 단서의 흔적을 따라가고 있으며 두 회사가 어떻게 해킹을 당했는지 이해하려고 노력하고 있습니다. 높은 수준에서 우리는 FireEye가 국가가 후원하는 적([state-sponsored adversary](https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html))에 의해 손상되었다는 것을 알고 있습니다. SolarWinds의 경우 공격자가 피해자의 네트워크에 9개월 동안 머무를 수 있었고 주요 용의자는 크렘린([Kremlin](https://www.reuters.com/article/global-cyber/u-s-homeland-security-thousands-of-businesses-scramble-after-suspected-russian-hack-idUSKBN28O1Z3))인 것으로 의심되고 있습니다.

의심할 여지없이 많은 조직이 의도적으로든 간접적으로든 공격에 포착되었는지 궁금해합니다. 다행히도 효과적인 위협 탐지 기능을 갖춘 기업은 FireEye, SolarWinds, Anomali 및 기타 위협 연구 기관이 제공하는 정보를 활용하여 공격을 받았는지 확인할 수 있습니다.

Anomali 고객은 이미 많은 위협 정보에서 앞서 있습니다. 전 세계가 공격을 인식하는 즉시 Anomali Threat Research는 Anomali ThreatStream에 알려진 침해 지표(IOC)의 포괄적인 목록과 함께 상황에 대한 상세하고 간결한 설명을 제공하는 위협 게시판을 즉시 업로드하여 사고와 관련된 정보(IOC, 보안 커뮤니티의 보고서, 서명 등)를 자동으로 고객에게 전달합니다. 이를 통해 EDR, 방화벽 및 SIEM을 포함한 보안 제어 전반에서 위협 탐지 및 차단을 자동화할 수 있습니다. 또한 당사의 위협 탐지 및 대응 제품인 Anomali Match를 사용하는 고객은 위협 인텔리전스를 사용하여 위협이 활성화된 시점으로 되돌아가 회귀 검색을 수행하여 위협이 네트워크에서 발견되었는지 여부를 보여주는 실시간 결과를 얻을 수 있습니다.

위협 인텔리전스 및 보안 운영 분석가에게 Anomali 위협 게시판이 어떻게 생겼는지 살펴볼 수 있도록 이 블로그에 FireEye 위협 게시판의 첫 번째 버전을 추가했습니다. Anomali 고객은 이 정보와 지속적인 업데이트를 사용하여 자신의 환경에서 관련 IOC의 존재를 감지하는 방법에 대해 확인할 수 있습니다. 자세한 내용은 당사로 문의하시기 바랍니다.

사건과 위협 인텔리전스가 탐지에 어떻게 도움이 되는지에 대한 심층적인 대화를 들으려면 이번 주 Anomali Detect 팟 캐스트([Anomali Detect Podcast](https://www.anomali.com/resources/podcasts/the-fireeye-solarwinds-hacks-adversaries-want-access-how-to-protect-your-organization))를 들어보십시오.



**Key Findings**

* 알려지지 않은 정교한 행위자가 지정되지 않은 날짜에 300개 이상의 FireEye Red Team 도구 및 대책(서명)을 훔쳤습니다.
* 워싱턴 포스트 익명의 출처는 Cozy Bear (APT29)가 책임이 있다고 주장했지만 증거를 제공하지 않았습니다.
* 행위자는 FireEye 고객, 특히 정부 기관에도 관심이 있었습니다.
* Red Team 대응책은 알려진 도구의 사용자 지정 버전, 우선 순위가 지정된 CVE (Common Vulnerabilities and Exposures) 목록 및 ClamAV, HXIOC, Snort 및 Yara 언어의 맬웨어 서명으로 구성되었습니다.
* 도난 당한 도구는 FireEye Red Team이 기존에 도구에 했던 것처럼 행위자에 의해 사용자 정의될 수 있습니다.

**Overview**

2020년 12월 8일, 미국에 기반을 둔 사이버 보안 회사인 FireEye는 정교한 위협 행위자가 Red Team(침투 테스트) 도구에 무단으로 액세스했다고 발표했습니다.[1] FireEye의 CEO인 Kevin Mandia는 국가 후원 행위자가 "세계적 수준의 기능"을 활용한 공격을 위해 특별히 FireEye를 표적으로 삼았다고 생각합니다.[2] 이 글을 쓰는 시점에서 사건이 발생한 특정 시간은 보고되지 않았습니다. 그러나 Thomson Reuters의 익명의 소식통은 회사가 지난 2주 동안 암호를 재설정했다고 주장했습니다.[3]

**Details**

알려지지 않은 날짜에 알려지지 않은 공격자들은 FireEye가 시뮬레이션 공격에 사용하는 300개 이상의 도구를 탈취하기 위해 상품과 새로운 기술의 조합을 사용했습니다.[4] 대책에는 사용자 지정 Red Team 도구, CVE 목록 및 ClamAV, HXIOC, Snort 및 Yara 언어로 된 수많은 서명이 포함됩니다.[5] 현재로서는 확인할 수 없지만 공격의 정교한 특성으로 인해 행위자가 절도를 하기 전에 정찰 단계를 수행했을 가능성이 매우 높습니다. 보안 침해에 대응하여 FireEye는 보안 기업이 이러한 Red Team 도구에 의해 발생하는 지속적인 위협이 될 가능성이 있는 것을 사전에 방어할 수 있도록 대책 서명을 공개했습니다.[6] Red Team 도구를 해킹하는 것 외에도, 행위자들은 FireEye의 정부 고객에 대해 더 많이 알고자 하는데 관심이 있는 것처럼 보였습니다.[7] 이는 이전의 Bit9, Kaspersky Lab 및 RSA 침해에서 관찰된 바와 같이 국가가 후원하는 행위자와 일치하는 전략입니다. 행위자는 당시 기존 보안 기능을 우회하는데 사용할 수 있는 정보를 탈취했습니다.[8]

Anomali Threat Research는 현재 사용 가능한 출처를 기반으로 속성을 결정할 수 없었지만, 다른 이들은 정부 고객에 대한 행위자의 관심으로 인해 러시아 정보 기관이 책임을 질 수 있다고 주장합니다. 워싱턴 포스트의 익명의 출처는 Cozy Bear (APT29, CozyDuke, TheDukes)가 공격의 배후에 있다고 주장했지만 이 주장을 뒷받침할 증거를 제공하지 않았습니다.[9]

Red Team 도구의 도난 외에도 행위자가 다른 회사에 관심이 있는 것으로 보이며, 이는 잠재적 인 향후 목표를 공격할 가능성이 높습니다. 그러나 FireEye가 언급한 이 공격 방식과 회사에 대한 특이성은 APT (Advanced Persistent Threat) 그룹 활동을 나타낼 수 있습니다. 따라서 행위자가 다른 목표에 대한 표지로 도구를 해킹했을 수도 있습니다. FireEye의 탐지 시그니처 릴리스는 Red Team을 수정하여 알려진 도구인 CobaltStrike 및 Metasploit과 유사함을 보여줍니다.[10] 행위자가 FireEye가 제안한 것처럼 정교하다면 이러한 도구를 사용하여 자신의 수정된 버전을 개발할 수 있습니다.

**Table 1** – CVE List Used by FireEye Red Team in Order of Priority[11]

| **CVE** | **Description** | **CVSS** |
| --- | --- | --- |
| CVE-2019-11510 | Pre-auth arbitrary file reading from Pulse Secure SSL VPNs | 10.0 |
| CVE-2020-1472 | Microsoft Active Directory escalation of privileges | 10.0 |
| CVE-2019-0604 | Remote code execution (RCE) for Microsoft Sharepoint | 9.8 |
| CVE-2019-0708 | RCE of Windows Remote Desktop Services (RDS) | 9.8 |
| CVE-2019-11580 | Atlassian Crowd Remote Code Execution | 9.8 |
| CVE-2019-19781 | RCE of Citrix Application Delivery Controller and Citrix Gateway | 9.8 |
| CVE-2020-10189 | RCE for ZoHo ManageEngine Desktop Central | 9.8 |
| CVE-2014-1812 | Windows Local Privilege Escalation | 9.0 |
| CVE-2019-3398 | Confluence Authenticated RCE | 8.8 |
| CVE-2020-0688 | RCE in in Microsoft Exchange | 8.8 |
| CVE-2016-0167 | Local privilege escalation on older versions of Microsoft Windows | 7.8 |
| CVE-2017-11774 | RCE in Microsoft Outlook via crafted document execution (phishing) | 7.8 |
| CVE-2018-8581 | Microsoft Exchange Server escalation of privileges | 7.4 |
| CVE-2019-8394 | Arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDesk Plus | 6.5 |

**Recommended Actions**

FireEye에서 제공하고 잠재적인 악성 활동을 모니터링하고 식별하는데 사용되는 모든 서명을 가져오는 것이 좋습니다. 또한 모범 사례에 따라 CVE 목록을 검토하고 필요한 경우 패치를 적용하는 것이 좋습니다. 잘 알려진 기업의 침해는 무기고를 위한 새로운 도구를 찾는 위협 행위자들로부터 높은 수준의 관심을 끌고 있습니다. 이 사건에 대한 지식과 FireEye가 제공하는 정보의 구현은 사전 방어에 도움이 됩니다.

**Endnotes**

[1] FireEye, “Unauthorized Access of FireEye Red Team Tools,” FireEye Blog, accessed December 11, 2020, published December 8, 2020, https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html; Kevin Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” FireEye Blog, accessed December 11, 2020, published December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html; Alexa King, “FORM 8-K: FireEye, Inc.,” United States Securities and Exchange Commission, accessed December 11, 2020, published December 8, 2020, https://www.sec.gov/ix?doc=/Archives/edgar/data/1370880/000137088020000037/feye-20201208.htm.

[2] Kevin Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” FireEye Blog.

[3] Christopher Bing and Joseph Menn, “U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools,” Thomson Reuters, accessed December 11, 2020, published December 8, 2020, https://www.reuters.com/article/us-fireeye-cyber/us-cybersecurity-firm-fireeye-discloses-breach-theft-of-hacking-tools-idUSKBN28I31E.

[4] FireEye, “Unauthorized Access of FireEye Red Team Tools,” FireEye Blog.

[5] “fireeye / red\_team\_tool\_countermeasures,” GitHub, accessed December 11, 2020, published December 8, 2020, https://github.com/fireeye/red\_team\_tool\_countermeasures.

[6] “fireeye / red\_team\_tool\_countermeasures,” GitHub.

[7] Dustin Volz and Robert McMillan, “U.S. Cyber Firm FireEye Says It Was Breached by Nation-State Hackers,” The Wall Street Journal, accessed December 11, 2020, published December 8, 2020, https://www.wsj.com/articles/u-s-cyber-firm-fireeye-says-it-was-breached-by-nation-state-hackers-11607461408; Greg Myre and Shannon Bond, “Top Cyber Firm, FireEye, Says It’s Been Hacked By A Foreign Govt.,” National Public Radio, accessed December 11, 2020, published December 8, 2020, https://www.npr.org/2020/12/08/944416183/top-cyber-firm-fireeye-says-its-been-hacked-by-a-foreign-govt.

[8] Christopher Bing and Joseph Menn, “U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools,” Thomson Reuters; Dustin Volz and Robert McMillan, “U.S. Cyber Firm FireEye Says It Was Breached by Nation-State Hackers,” The Wall Street Journal.

[9] Ellen Nakashima and Joseph Marks, “Spies with Russia’s foreign intelligence service believed to have hacked a top American cybersecurity firm and stolen its sensitive tools,” The Washington Post, accessed December 11, 2020, published December 8, 2020, https://www.washingtonpost.com/national-security/leading-cybersecurity-firm-fireeye-hacked/2020/12/08/a3369aaa-3988-11eb-98c4-25dc9f4987e8\_story.html.

[10] Lucian Constantin, “FireEye breach explained: How worried should you be?” CSO Online, accessed December 11, 2020, published December 10, 2020, https://www.csoonline.com/article/3600893/fireeye-breach-explained-how-worried-should-you-be.html.

[11] “fireeye / red\_team\_tool\_countermeasures,” GitHub.