POINT
OF VIEW

Recorded Future®

By John Wetzel

POV-2020-1230

SolarWinds 원점추적:

우리는 앞서 가고 있는가?

UNC2452 정보 분석

참고: 이 보고서의 이전 버전에서 Jake Williams의 미국 NSA(National Security Agency) TAO(Tailored Access Operations) 그룹 소속 활동을 Sandworm이 폭로했다는 것은 잘못된 내용이다. 이 폭로는 ShadowBrokers에 의해 실행되었다.

개요

최근 SolarWinds Orion 플랫폼에서 악성 백도어를 통해 6개 이상의 정부기관과 아직 알려지지 않은 여러 조직들을 대상으로 한 광범위한 침입 캠페인이 발생했다. 이 캠페인은 이미 역사상 가장 중대한 사이버 스파이 행위 중 하나로 등극했다. SUNBURST/Solorigate라고 불리는 이 침입은 파괴가 아닌 정보 유출 및 첩보 활동을 목적으로 하는 것으로 보인다. 따라서 사고 대응 뿐만 아니라 방첩 활동(counterintelligence) 분야에서도 이 캠페인을 주시하고 있다. 방첩 활동 측면에서 이 사건을 분석함으로써 네트워크 방어자들에게 혼란을 가중시킬 수 있는 복잡한 분석보다는 이 사건에 대한 기술형 언어(descriptive language)의 공백을 채울 수 있다. 또한 백도어의 기술적 구성요소에 대한 유의미한 인사이트를 얻기 위해 직접 액세스하고 조사할 수 있는 리소스를 보유한 있는 기업은 소수에 불과하다. 배후의 행위자(actor)는 별개의 문제이다.

대부분의 복잡한 공공기관 대상 침입들과 마찬가지로 이번 사건의 배후도 지저분하게 얽혀있다. FireEye는 이번 침입의 배후에 있는 행위자를 'UNC2452'로 명명했으며, Volexity는 이 위협 행위자를 'Dark Halo'라고 불렀다. Volexity는 Dark Halo가 UNC2452와 동일하다고 했으나 FireEye는 이에 대한 구체적인 확인을 내놓지 않았다. 워싱턴 포스트 특파원 Ellen Nakashima는 익명의 정부 소식통을 인용하여 이번 공격이 러시아계 행위자, 특히 APT29의 소행일 것이라는 주장을 보도했다. 미 의회 의원들도 러시아, 특히 러시아 해외정보국(Russian Foreign Intelligence Service, SVR)을 책임 당사자로 공개적으로 비난하고 대응을 촉구했다. Microsoft 사장인 Brad Smith도 강력한 행동을 촉구했다. 이들 조직은 기밀 소스는 물론 이번 침해의 성격에 대해 훨씬 더 많은 정보를 갖고 있을 것이다. 하지만 강력한 대응을 요구하기 위해서는 비난을 뒷받침할 수 있는 공개된 정보가 필요하다.

이러한 주장에 대한 공개 증거는 현재 부족한 상황이다. Rendition Security를 운영하고 SANS Institute에서 강의 중인 Jake Williams는 기술적 증거가 곧 나오겠지만 이를 공개하면 결국 적에게 실수를 알려주고 흔적을 숨길 수 있는 수단을 제공할 수 밖에 없다고 말했다. 공개된 증거의 부족으로 인해 다른 위협 행위자들, 심지어 다른 국가들에 대한 배후설도 제기되고 있다. 이는 도널드 트럼프 대통령의 주장이기도 하다.

정확한 정보 분석을 위해서는 편견이 배제되어야 한다. 편견은 정책의 실수로 이어질 수 있다. 명백한 증거 없이 상대적 대응(또는 때로는 불균형 대응)에 대한 정책을 논의하는 것은 위험할 수 있다. 러시아 배후설이 유포되고 있는 상황에서 근거에 앞서 주체를 단정하는 것은 시기상조이자 근시안적인 판단이며, 보안 분석가를 특정 활동과 행위자에게만 편향시킨다. 또한 정보 분석은 대응에 대한 전략적, 전술적 지침을 제공한다. 전략적 차원에서 대응은 잘 조직되고 상대적이어야 한다. 전술적 차원에서는 방어자가 정보를 기반으로 선제적 조치(예: 예행 연습이 확인된 이후의 위협 헌팅)에 착수할 수 있다.

정보보안 연구원들 사이에서 APT41과 같은 그룹이 이번 침입의 주체일 수 있다는 논의가 있었다. Winnti 및 Barium이라고도 알려진 APT41은 중국계 해커 그룹으로 과거 SUNBURST/Solorigate 공격과 비견되는 공격을 수행한 전력이 있다. (참고: 레코디드 퓨처는 APT41, Axiom Hacking Group, Barium, Blackfly, Dogfish, Ragebeast, Wicked Panda, Winnti Group, Winnti Umbrella Group 등 여러 그룹명을 동의어로 써왔다.) 2017년 3월 APT41이 시스템 클리너 소프트웨어인 CCleaner를 만든 회사에 침투하여 공급망 공격을 자행했다. Cisco Talos와 Morphisec의 연구원들이 이 캠페인을 발견했으며, 이 캠페인은 결국 227만 대의 컴퓨터를 감염시켰다. 이러한 비교만으로 배후를 단정하기는 어렵지만 APT41을 SUNBURST/ Solorigate 공격의 후보 그룹으로 고려할만한 가치는 있다.

주목할만한 기술

우리는 원점추적(attribution)과 공격자 매핑(adversary mapping)에 초점을 맞추기 위해 기존 기술을 사용하여 분석에 접근했다. 공격자의 동기와 의도에 대한 인사이트를 제공하기 위해 MITRE ATT&CK 기술 매핑, 피해 대상 조사, 시간적 징후, 히스토릭 지표의 사용을 포함한 방법론을 따랐다. 이 캠페인의 고유한 특징을 파악하기 위해 공개 정보와 레코디드 퓨처의 히스토릭 인덱스(historic index)를 모두 분석하였다. 우리의 목표는 이 공격의 주체를 확정하는 것이 아니라 정보 분석을 통해 기존 데이터를 검토하고 공격자 추적에 대한 논의에 기여하는 것이다.

ATT&CK 기술 분석

우리는 APT29와 APT41을 포함하여 언급된 행위자들의 ATT&CK 기술을 비교했다. FireEye와 Microsoft의 보고서에 언급된 기술과 MITRE ATT&CK Matrix for Enterprises를 사용하여 UNC2452에 대한 25개 기술과 14개 하위 기술을 컴파일했다. 그런 다음 그룹 비교를 위한 MITRE 지침을 기반으로 ATT&CK Navigator를 사용하여 UNC2452 ATT&CK 기술과 APT29 및 APT41에 대해 MITRE 팀이 문서화한 기술을 비교했다(부록 참조). 안타깝게도 우리의 분석은 몇 가지 문제를 드러냈다.

첫째, 동일한 행위자 그룹 및/또는 멀웨어를 분석하는 데 있어서 벤더들 간에 문서화된 ATT&CK 기술에 상당한 차이가 있었다. 예를 들어 FireEye의 2020년 12월 13일 보고서에는 7가지 기술과 10가지 하위 기술이 나열되어 있다. Microsoft의 2020년 12월 18일 보고서에는 4가지 기술과 6가지 하위 기술이 나온다.

둘째, APT29과 APT41의 몇몇 기술들이 MITRE가 분류한 ATT&CK 그룹에 누락되어 있다. PowerDuke 캠페인과 같은 최근의 공격에 치우쳐 있는 것으로 보인다. 우리는 초기 비교를 위해 MITRE의 APT TTPs 목록을 사용했으나, 멀웨어 기술과 해당 멀웨어를 활용하는 행위자 그룹의 기술에도 현저한 차이가 있는 것으로 보인다.

셋째, 보안 리포팅에 설명된 미묘한 일치 기술이 ATT&CK에 없는 경우가 있었다. 예를 들어, ATT&CK Navigator에서 T1078 Valid Accounts와 같은 몇 가지 기술이 자동으로 전술에 대입되며, 이는 Initial Access, Persistence, Defense Evasion에 대입된다. Microsoft는이 기술을 언급하지만 Persistence 전술에 대한 적용 가능성을 제한한다.

또한 일부 기술은 반복되는 적용과 인코딩 대상 선택으로 의미가 있다. Salt 값을 첨가한 FNV-1a 해싱 알고리즘은 T1132 Data Encoding에 해당하는 블랙리스트 도메인과 블랙리스트 프로세스 모두에 사용된다. 그러나 FNV-1a로 해시된 도메인은 2단계 페이로드를 다운로드하기 전에 검사에서 다양한 정보 구성 요소를 표준화하는 데도 사용되어 통신 효율성과 난독화를 제공한다.

ATT&CK은 공격자 TTPs 매핑을 위한 강력한 프레임웍이지만 진행 중인 공격 활동을 설명하고 해당 활동을 과거 활동에 매핑하는 데 필수적인 요소가 빠져있다. 인라인 컨텍스트가 없는 ATT&CK 기술의 벤더 발표는 공격자 매핑에 대한 적용을 더욱 어렵게 만든다. 활동 히스토리 추적은 기존 및 진행 가능성이 있는 SUNBURST/Solorigate 캠페인에 대한 인사이트와 행위자 동기 및 속성에 대한 단서를 제공할 수 있다.

피해 대상

UNC2452는 엄격한 방식으로 타겟을 선별하면서 작업을 진행하기 때문에 특히 피해 대상에 주목할만하다. Microsoft 사장 Brad Smith의 성명에 따르면, 백도어가 포함된 SolarWinds 업데이트를 받은 약 18,000개 조직 중에서 2단계로 넘어간 비율은 단 0.2%에 불과했다. 그리고 이 선택된 기업 중 80%에 해당하는 40개 기업이 미국에 있었다. FireEye에 따르면 공격자는 각 피해 대상에게 맞춤화된 DGA(domain generation algorithms)를 사용하여 패시브 DNS 레코드를 통해 백도어 C2 서버로 신호를 보내는 조직을 식별하고 인코딩된 서브도메인을 크래킹한다.

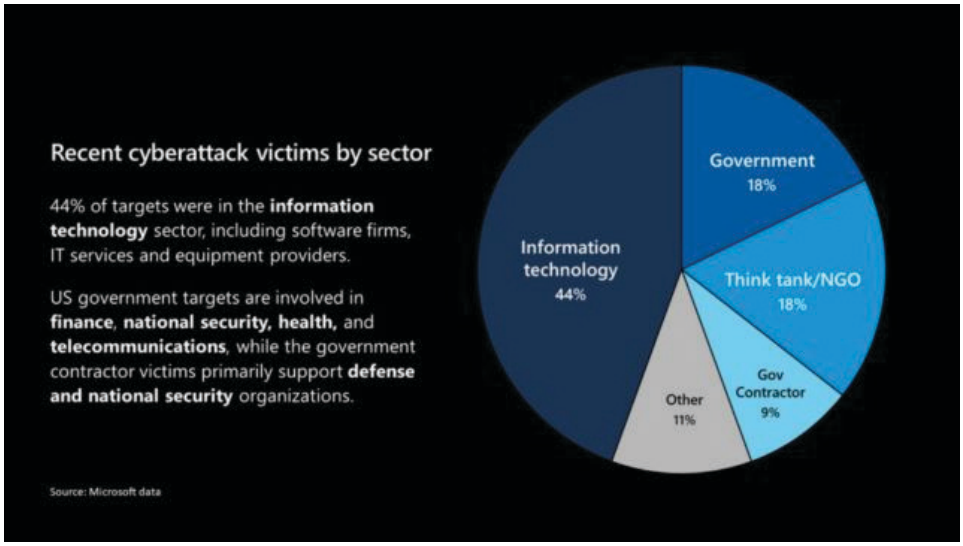


그림 1: Microsoft가 확인한 산업별 피해 대상 (출처: Microsoft)

Microsoft에 따르면 비해 피해 대상의 대다수가 IT 기업이다. 여태까지 언론에서는 정부기관과 정부 계약업체들의 피해를 중점적으로 보도했으나, 최근 보고된 바에 따르면 통신사업자에서 의료기관에 이르기까지 전통적인 국가 첩보 행위 대상을 넘어선 표적을 노렸음을 확인할 수 있다.

일부 피해 대상은 Solorigate 백도어에서 사용하는 DGA를 역으로 하여 확인할 수 있다. RedDrip Team, Netresec, Kaspersky 등이 백도어에서 초기 C2 통신에 사용하는 DGA를 디코딩하는 방법을 공개했다. 레코디드 퓨처는 Pastebin, pDNS(passive DNS datasets), 기타 SolarWinds Orion 백도어 1단계 C2 도메인 avsvmcloud[.]com의 인코딩된 서브도메인과 관련된 오픈소스 정보를 수집하고 통합했다. 그리고 3개의 DGA 디코딩 스크립트를 활용했다. 2020년 12월 21일 기준으로 우리가 파악한 도메인은 약 286개이다.

이 아웃풋은 오픈소스 데이터의 작은 부분 집합 결과이며 영향을 받는 조직들 전체를 나타내지 않는다. 그리고 현 시점에서 오픈소스 데이터 세트를 통한 레코디드 퓨처의 가시성만을 기반으로 한다. SolarWinds는 약 18,000개 조직이 SUNBURST의 영향을 받는 SolarWinds Orion 소프트웨어 버전을 설치했다고 말했다. 따라서 레코디드 퓨처가 파악한 도메인 목록은 포괄적인 것이 아니다. 또한 이 목록에 있는 조직이 반드시 2단계 감염 또는 데이터 유출의 피해자임을 의미하지는 않는다. 멀웨어가 2단계를 실행하려면 특정 조건이 충족되어야 했다. 우리는 현재 더 이상의 익스플로잇에 대한 가시성이 없다. 모든 레코드가 완전한 도메인은 아니다. 해당 도메인이나 스트링과 관련된 조직을 경험에 의한 추측이나 추론으로 짐작하기에 충분한 정보가 있다고 판단되는 부분적이거나 불완전한 도메인을 포함시켰다.

Microsoft는 보고서에서 멀웨어가 실행 전에 도메인에서 특정 문자열을 검사한다고 밝혔으나, 해시로 구현된 까닭에 도메인을 확인하지는 못했다. Checkpoint 보안 연구원인 Itay Cohen은 해당 문자열을 FNV-1a 해시로 파악하고 이를 역으로 무차별 대입할 수 있었다. Cohen은 많은 문자열이 SolarWinds 내부 도메인 네임으로 보인다고 지적했다. Cohen은 멀웨어가 "solarwinds" 및 "test"의 정규 표현을 찾기 위한 검사를 수행한 것과 관련하여 공격자가 발각 위험을 최소화기 위해 네트워크 토폴로지, 내부 개발 도메인 네임은 물론 SolarWinds 소스코드에 대한 상세한 정보를 수집했을 것으로 단정했다. Costin Raiu는 다른 Kaspersky 연구원과 함께 나머지 해시를 해독하여 내부 도메인 네임 전체 목록을 게시했다. 탐지를 피하기 위한 공격자의 이러한 조심성은 매우 드문 경우이며, 고도의 정찰과 집중력을 보여준다.

```
OrionImprovementBusinessLayer.patternHashes = new ulong[]
{
    //HASH                      //domain:
    1109067043404435916UL,      //[dev.local]
    15267980678929160412UL,     //[swdev.dmz]
    838129226599397726UL,       //[lab.local]
    379640562369566524UL,       //[lab.na]
    872747776954430206UL,       //[emea.sales]
    1073412700424487970UL,      //[cork.lab]
    1107328331110454169UL,      //[dev.local]
    403023641397519965UL,       //[dmz.local]
    770168327982439773UL,       //[pci.local]
    513225662010499863UL,       //[saas.swi]
    594228205252529491UL,       //[lab.rio]
    457848084625562946UL,       //[lab.brno]
    168589559781464066UL        //[apac.lab]
};
```

그림 2: FNV-1a 해시 및 SUNBURST 멀웨어가 회피한 도메인 네임

이어서 SentinelOne이 SUNBURST가 특정 실행 프로세스를 검사하고 해당 프로세스를 발견하면 종료된다는 것을 알아냈다.

> *"SearchConfigurations()는 블랙리스트 드라이버를 식별하는 데 사용된다. 이 작업은 WMI query - Select * From Win32_SystemDriver 를 통해 실행된다(아래 스크린샷에서 C07NSU0uUdBScCvKz1Ulz8wzNooPriwuSc11KcosSy0CAA==으로 난독화됨). 각 드라이버에 대한 파일 네임을 가져오고, 이 드라이버가 블랙리스트에 있으면 이 메소드는 true를 리턴한다. 앞서 언급했듯이 true를 리턴하면 멀웨어가 true 백도어 코드를 실행하기 전에 Update() 루프를 이탈하게 된다."*

블랙리스트 프로세스 중에는 많은 디지털 포렌식 및 엔드포인트 탐지 및 대응 도구가 있다. 드라이버 전체 목록은 SentinelOne 블로그에서 확인할 수 있다. 블랙리스트 도메인에 대한 Microsoft의 폭로와 마찬가지로, 엔드포인트 탐지를 회피하기 위한 이러한 노력은 행위자의 신중함을 보여준다.

또한 SUNBURST 블랙리스트 프로세스 목록에 대한 분석이 필요하다. 전체 목록은 여러 오픈소스 연구원들에 의해 크래킹되었다. Royce Willams와 Hashcat 팀이 공개 Google Sheet를 작성하였다. 이러한 블랙리스트 프로세스 목록에 일반적인 엔드포인트 또는 안티바이러스 벤더들이 모두 포함되어 있지는 않다. 멀웨어 개발자가 특정 엔드포인트 소프트웨어만 블랙리스트에 올린 이유를 파악하기 위해서는 추가 분석이 필요하다.

시간

Solorigate 백도어의 특징은 DLL 마지막 쓰기 시간(the last write time)이 12-14일 이전인 타임스탬프 체크이다. 멀웨어 샘플들 중에서도 이러한 기간은 이례적이다. MITRE ATT&CK에 이 기술을 활용하는 소수의 공격자가 나열되어 있으며, 이 정도 시간에 근접한 공격자는 없지만 앞서 언급한 것처럼 ATT&CK에서 완전히 문서화되지 않았기 때문일 수 있다. 시간 기반 회피는 가상화/샌드박스 분석 보다는 SolarWinds 직원의 탐지를 피하기 위한 것으로 보인다.

이 캠페인은 2019년 가을 SolarWinds를 침해하여 코드를 변경시킨 것으로 보인다. 이러한 비악성 변경(non-malicious changes)은 2020년 3월에 발생한 1차 감염의 예행 연습에 해당한다. 또한 공격자들은 대상 DLL 파일의 크기를 500k에서 900k로 늘렸다. 이로 인해 탐지 규칙이 트리거되었더라도 조사에서 악성 코드가 발견되지 않았을 것이다. 2020년 2월/3월에 감염된 코드가 추가되었을 때 파일 크기 증가는 미미했다. 여러 달에 걸쳐 이러한 준비 작업을 진행했다는 것은 정보 수집 작전 수준의 엄격한 조직력과 인내심을 보여준다.

히스토릭 지표

FireEye 및 기타 벤더 보고서에서 여러 지표가 공유되었다. 이러한 지표 중 다수가 이 공격과 관련해 새로운 것이지만, 레코디드 퓨처는 이러한 지표 중 일부에 대한 히스토릭 레퍼런스를 갖고 있다.

레코디드 퓨처는 이 보고서에서 세 가지 도메인에 대한 히스토릭 컬렉션을 확인한다.

- 도메인 freescanonline[.]com은 2017년 11월 28일 ReversingLabs 스캔에서 최초로 확인되었으며 다음의 SHA256 해시와 연관되었다.
  21bab0d279d15a548a84a9d9eed34575b2dc9072cc36ebfe7b517850eea92756.
- 이 도메인은 2019년 10월 13일 추가적인 ReversingLabs 스캔에서도 확인되었으며 다음의 SHA256 해시와 연관되었다.
  c5864330c247e2cd2a98d69b852e42f59a16d9613a6536c8b0b25e16c934533d.
- 도메인 highdatabase[.]com은 "NII GSOC Advisory"라는 제목으로 2020년 12월 10일 Pastebin 사이트에 공개적으로 포스팅되었다.

FireEye 보고서에 언급된 10개의 IP 주소 중에서 단 3개만이 이전 악성 행위와 연계되어 있었다.

- 13[.]59[.]205[.]66은 2018년 2월 6일 Pastebin에 처음 등장했으며, 2019년 4월 23일 URLScan 목록에 악성 호스트로 올라왔다. https://urlscan.io/result/3df2efd6-530f-4973-bca7-4635c083e276
- 139[.]99[.]115[.]204는 2019년 6월로 거슬러 올라가는 두 개의 URLScan 결과에 언급되었다. 2019년 12월에 이 IP 주소가 NAO_sec 보고서에서 언급되었는데 일본을 겨냥한 Bottle Exploit Kit라는 도구와 sales[.] inteleksys[.]com 도메인이 연계되어 있었다.
- 167[.]114[.]213[.]199는 이전에 Bambenek 목록에 DGA 도메인 목적지로 올라와 있었다. 또한 SolarWinds 사태 발표 며칠 전에 이 IP에 대해 레코디드 퓨처의 Predictive IP Risk Rule이 트리거되었다.

FireEye가 언급한 기술 외에도, Microsoft는 "Solorigate" 백도어에 대한 보고서에서 이 캠페인과 관련된 5개의 추가적인 기술과 1개의 하위 기술을 설명했다.

Execution

- T1072 Software Deployment Tools

Command and Control

- T1071.004 Application Layer Protocol: DNS
- T1132 Data Encoding

Defense Evasion

- T1480.001 Execution Guardrails: Environmental Keying
- T1562.001 Impair Defenses: Disable or Modify Tools

Collection

- T1005 Data From Local System

DomainTools는 공개된 DNS 레코드 관점에서 주제에 접근한 두 개의 블로그를 게시했다. FireEye가 게시한 DNS 레코드 문서화 외에 2단계 페이로드 딜리버리에 사용된 추가 도메인도 게시되었다.

Domain	Create Date	IP	Hosting Provider	SSL/TLS Certificate
databasegalore.com • 69	2019-12-14	5.252.177.21 • 79	MivoCloud SR	d400021536d712cb
digitalcollege.org • 75	2019-03-24	13.57.184.217 • 27	Amazon Technologies Inc.	fdb879a2ce7e2cda2
ervsystem.com • 10	2018-02-04	198.12.75.112 • 5	ColoCrossing	0548eedb3d1f45f1f
globalnetworkissues.com • 72	2020-12-16	18.220.219.143 • 72	Amazon Technologies Inc.	ff883db5cb023ea6b
incomeupdate.com • 72	2016-10-02	5.252.177.25 • 78	MivoCloud SRL	4909da6d3c809aee
infinitysoftwares.com • 5	2019-01-28	107.152.35.77 • 0	ServerCheap INC	e70b6be294082188
kubecloud.com • 69	2015-04-20	3.87.182.149 • 73	Amazon Data Services NoVa	1123340c94ab0fd1
lcomputers.com • 74	2002-01-27	162.223.31.184 • 5	QuickPacket LL	7f9ec0c7f7a23e565
panhardware.com • 74	2019-05-30	204.188.205.176 • 79	SharkTech	3418c877b4ff052b6
seobundlekit.com • 74	2019-07-14	3.16.81.254 • 73	Amazon Technologies Inc	e7f2ec0d868d84a33
solartrackingsystem.net • 73	2009-12-05	34.219.234.13 • 0	Amazon Technologies Inc.	91b9991c10b1db51
virtualwebdata.com • 73	2014-03-22	18.217.225.111 • 72	Amazon Technologies Inc.	ab93a66c401be78a
webcodez.com • 73	2005-08-12	45.141.152.18 • 5	M247 Europe SRL	2667db3592ac3955
zupertech.com • 74	2016-08-16	51.89.125.18 • 78	OVH SAS	d33ec5d35d7b0c23

그림 3: 후속 단계에서 사용되는 DomainTools 도메인 스크린샷. Recorded Future Express Plus Browser Extension으로 강화 (2020년 12월 20일)

이러한 2단계 도메인 중 일부는 인덱스에서 도메인 등록과 인증서 등록 레퍼런스 사이에 상당한 지연이 나타난다.

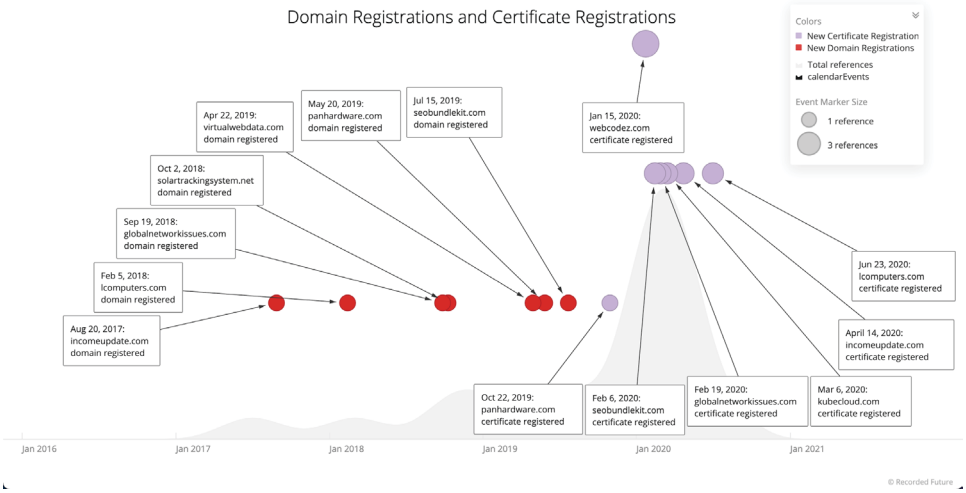


그림 4: 도메인 등록과 인증서 등록 지연 타임라인. (출처: Recorded Future)

globalnetworkissues.com mentioned

SEP 19 2018

Translated from : "New domain registration for globalnetworkissues.com"
Translated from : **"The domain globalnetworkissues.com has been registered"**
Show original
Source New Domain Registrations on Sep 19, 2018, 00:00 • Reference Actions • 1+ reference

CertificateRegistration

FEB 19 2020

Certificate Registration
"A certificate for the domain **globalnetworkissues.com** has been registered"
Source New Certificate Registrations on Feb 19, 2020, 17:58 • Reference Actions • 2+ references

그림 5: globalnetworkissues[.]com의 도메인 등록 및 인증서 등록 날짜를 보여주는 레퍼런스 (출처: Recorded Future)

2018년 9월 19일에 globalnetworkissues[.]com의 등록이 확인되었으나 17개월 후인 2020년 2월 19일까지 TLS 인증서 등록이 이루어지지 않았다.

incomeupdate.com mentioned

AUG 20 2017

New domain registration for incomeupdate.com
"The domain **incomeupdate.com** has been registered"
Source New Domain Registrations on Aug 20, 2017, 00:00 • Reference Actions • 1+ reference

CertificateRegistration

APR 14 2020

Certificate Registration
"A certificate for the domain **www.incomeupdate.com** has been registered"
Source New Certificate Registrations on Apr 14, 2020, 10:54 • Reference Actions • 2+ references

그림 6: incomeupdate[.]com의 도메인 등록 및 인증서 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2017년 8월 20일에 incomeupdate[.]com 등록이 확인되지만 거의 19개월 후인 2020년 4월 14일까지 TLS 인증서 등록이 이루어지지 않았다.

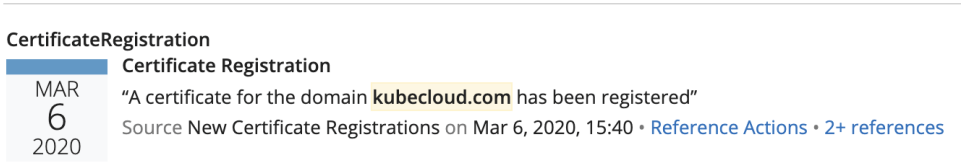


그림 7: kubecloud[.]com 도메인의 인증서 등록 날짜를 보여주는 레퍼런스 (출처: Recorded Future)

2020년 3월 6일에 kubecloud[.]com에 대한 TLS 인증서 등록이 확인된다.

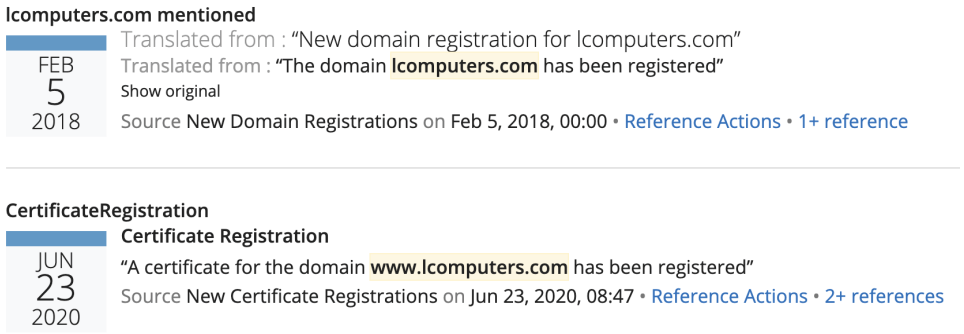


그림 8: lcomputers[.]com의 도메인 등록 및 인증서 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2018년 2월 5일에 lcomputers[.]com 등록이 확인되지만 2020년 6월 23일까지 TLS 인증서 등록이 이루어지지 않았다.

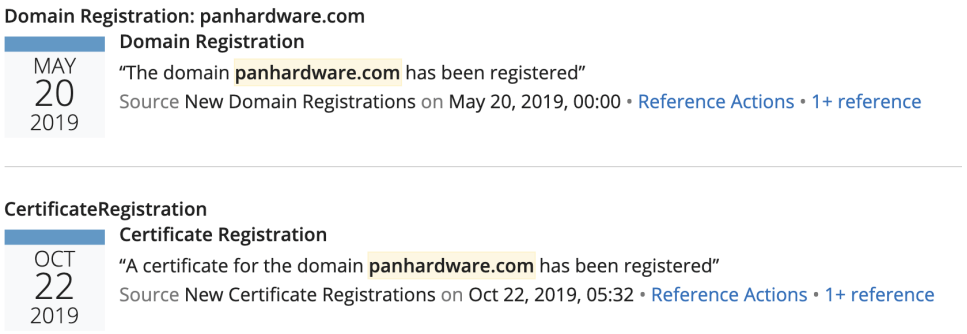


그림 9: panhardware[.]com의 도메인 등록 및 인증서 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2019년 5월 20일에 panhardware[.]com이 등록되고 5개월 후인 2019년 10월 22일에 인증서가 등록된 것으로 확인된다. 다른 2단계 도메인에 비해 훨씬 앞선 이 등록은 흥미로운 케이스이며 추가 조사할 가치가 있다.

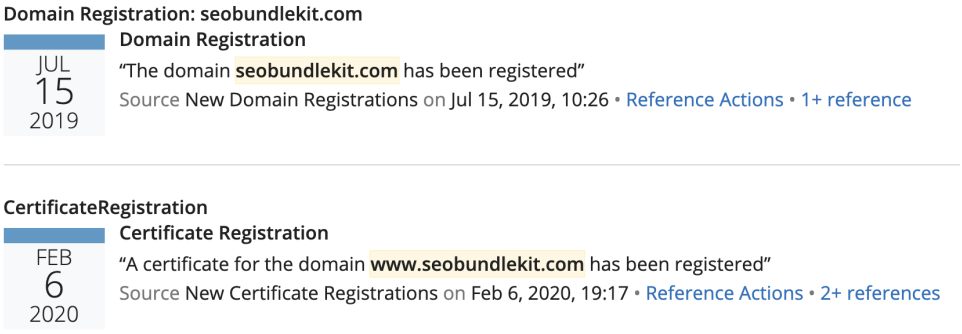


그림 10: seobundlekit[.]com의 도메인 등록 및 인증서 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2019년 7월 15일에 seobundlekit[.]com 등록이 확인되지만 2020년 2월 6일까지 TLS 인증서 등록이 이루어지지 않았다.

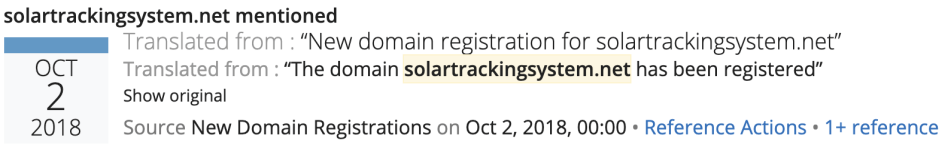


그림 11: solartrackingsystem[.]com 도메인 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

이 도메인과 다음 두 도메인의 경우 도메인 등록 또는 인증서 등록에 대한 레퍼런스가 확인되지만 둘 다는 아니다. 2018년 10월 2일 solartrackingsystem[.]net이 등록되었으나 TLS 인증서 등록은 확인되지 않는다. TLS 인증서가 없다고 해서 인증서 자체가 없음을 나타내는 것은 아니다. DomainTools에 이 도메인에 대한 인증서가 나오기 때문이다. 이는 해당 기간 인증서 등록에 대한 우리의 적용 범위에 누락이 있을 가능성이 높다.

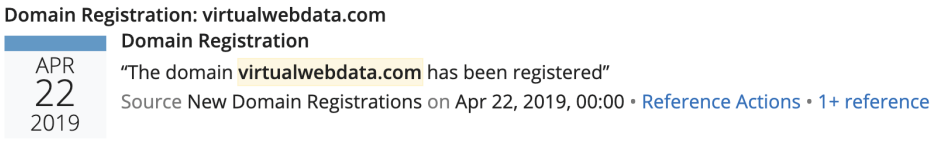


그림 12: virtualwebdata[.]com 도메인 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2019년 4월 22일 virtualwebdata[.]com 등록이 확인되나 TLS 인증서 등록은 확인되지 않는다.

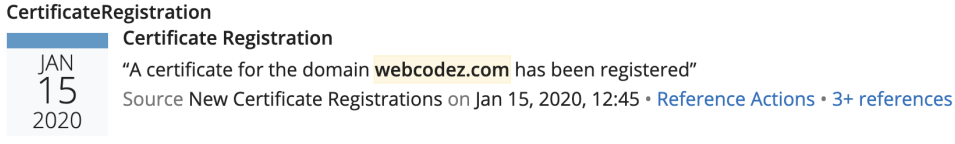


그림 13: webcodez[.]com 도메인 인증서 등록 날짜를 보여주는 레퍼런스. (출처: Recorded Future)

2020년 1월 15일 webcodez[.]com 등록이 확인되나 TLS 인증서 등록은 확인되지 않는다. 이것은 이 도메인 집합에서 확인되는 가장 최근 등록 중 하나이다.

도메인 등록과 인증서 등록 사이의 이러한 지연은 공격자가 나중에 사용하려고 이러한 도메인을 맡아 두었음을 시사한다. 그러므로 UNC2452 행위자에 ATT&CK 하위 기술인 T1583.001 Acquire Infrastructure: Domains를 추가할 것을 제안한다.

DomainTools 보고서의 2단계 도메인과 관련된 3개의 IP 주소는 이전에 레코디드 퓨처에서 확인되었다. IP 주소 13[.]57[.]184[.]217 및 198[.]12[.]75[.]112는 각각 2018년 4월 6일과 2020년 3월 19일에 abuseipdb.com에 보고되었다. IP 주소 3[.]16[.]81[.]254는 2019년 1월 20일에 포스팅된 Pastebin 게시물에서 처음 발견되었다.

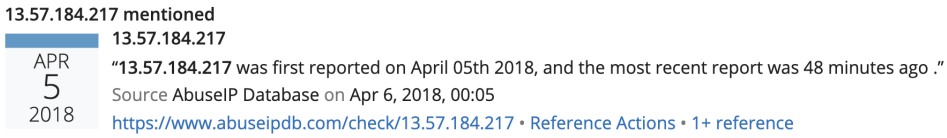


그림 14: 2018년 4월 6일에 AbuseIP Database에 올라온 IP 주소 13[.]57[.]184[.]217을 보여주는 레퍼런스. (출처: Recorded Future)

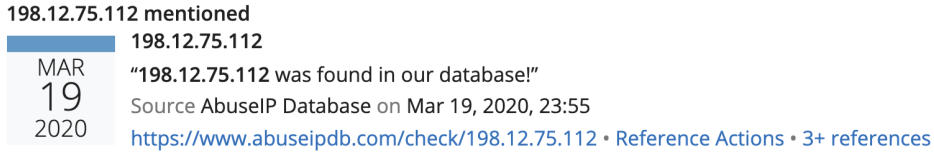


그림 15: 2020년 3월 19일 AbuseIP Database에 올라온 IP 주소 198[.]12[.]75[.]112을 보여주는 레퍼런스. (출처: Recorded Future)

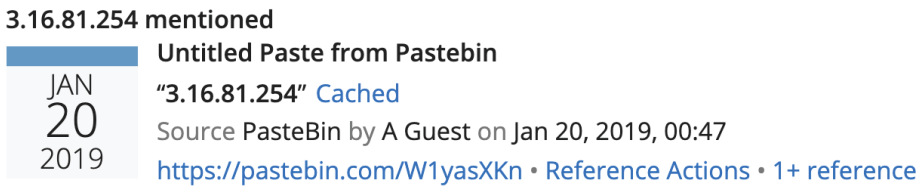


그림 16: 2019년 1월 20일에 PasteBin에 올라온 IP 주소 3[.]16[.]81[.]254을 보여주는 레퍼런스. (출처: Recorded Future)

45[.]141[.]152[.]18은 Urlscan.io. 사이트의 여러 스캔에서 확인된다. 또한 이 IP 주소는 2020년 7월 19일 레코디드 퓨처 히스토릭 위협 리스트인 Recent Hosts of DDNS Names에 나타났다.

행위자가 다수일 가능성

Microsoft는 또한 SolarWinds Orion 제품에 영향을 미치는 것으로 밝혀진 두 번째 멀웨어에 대한 조사 내용을 발표했다. 이 멀웨어가 Solorigate 백도어와 관련이 있는지 혹은 또 다른 위협 행위자를 나타내는지 여부는 확인되지 않았다. Microsoft 블로그의 부록 섹션에 나온 내용은 다음과 같다.

> *"SolarWinds 침해 전반에 대한 조사에서 SolarWinds Orion 제품에 영향을 미치는 멀웨어가 추가로 발견되었으나, 이것은 이번 침해와 관련이 없으며 다른 위협 행위자가 사용한 것으로 확인되었다. 해당 멀웨어는 App_Web_logoimagehandler.ashx.b6031896.dll이라는 DLL 파일 형태의 소형 Persistence Backdoor로 구성되며 "inetpub\SolarWinds\bin\" 폴더에 설치되면 SolarWinds 웹 애플리케이션 서버를 통해 원격 코드 실행을 허용하도록 프로그래밍되어 있다. Solorigate와 달리 이 악성 DLL에는 디지털 서명이 없어서 공급망 공격과 무관한 것으로 보인다."*

Microsoft, GuidePoint, Palo Alto Networks는 이 두 번째 멀웨어 .NET Webshell의 이름을 SUPERNOVA로 명명했다. SUPERNOVA가 악성 Powershell 스크립트인 CosmicGale을 로딩하는 것으로 생각된다. Microsoft는 SolarWinds 설치에서 SUPERNOVA가 탐지되면 별도의 감염으로 처리해야 한다고 권고한다. 확정적인 것은 아니지만 이 추가 멀웨어는 동일한 환경에서 다수의 위협 행위자가 존재할 가능성을 제기한다. 동일 시스템에서 알게 모르게 다수의 위협 행위자가 암약하는 것은 어제 오늘 일이 아니다. 일례로 APT28과 APT29의 증거는 2016년 침해된 미국 DNC(Democratic National Committee) 서버에서 발견되었다. 또한 ShadowBrokers 릴리즈에서 유출된 파일은 다른 공격 감염을 스캔하는 데 사용할 수 있는 45개의 파일 시그니처를 보여주었다. 이 가운데 일부는 당시 알려지지 않은 공격이었다. 이 또한 여전히 배후 집단을 확정하기 어렵다는 주장에 힘을 실어준다.

결론

Virus Bulletin 2018 컨퍼런스에서 보안 전문가 Juan Andres Guerrero-Saade는 다음과 같이 말했다. "현재 우리가 알고 있는 것은 '이 행위자가 정교한가, 아닌가?' 둘 중 하나로 귀결된다." 이 새로운 캠페인에 대한 수많은 언론 해설에서 알 수 있듯이 변한 것은 별로 없다. 우리는 일반적인 속성과 현재의 특징을 좀 더 자세히 조사하고자 했다.

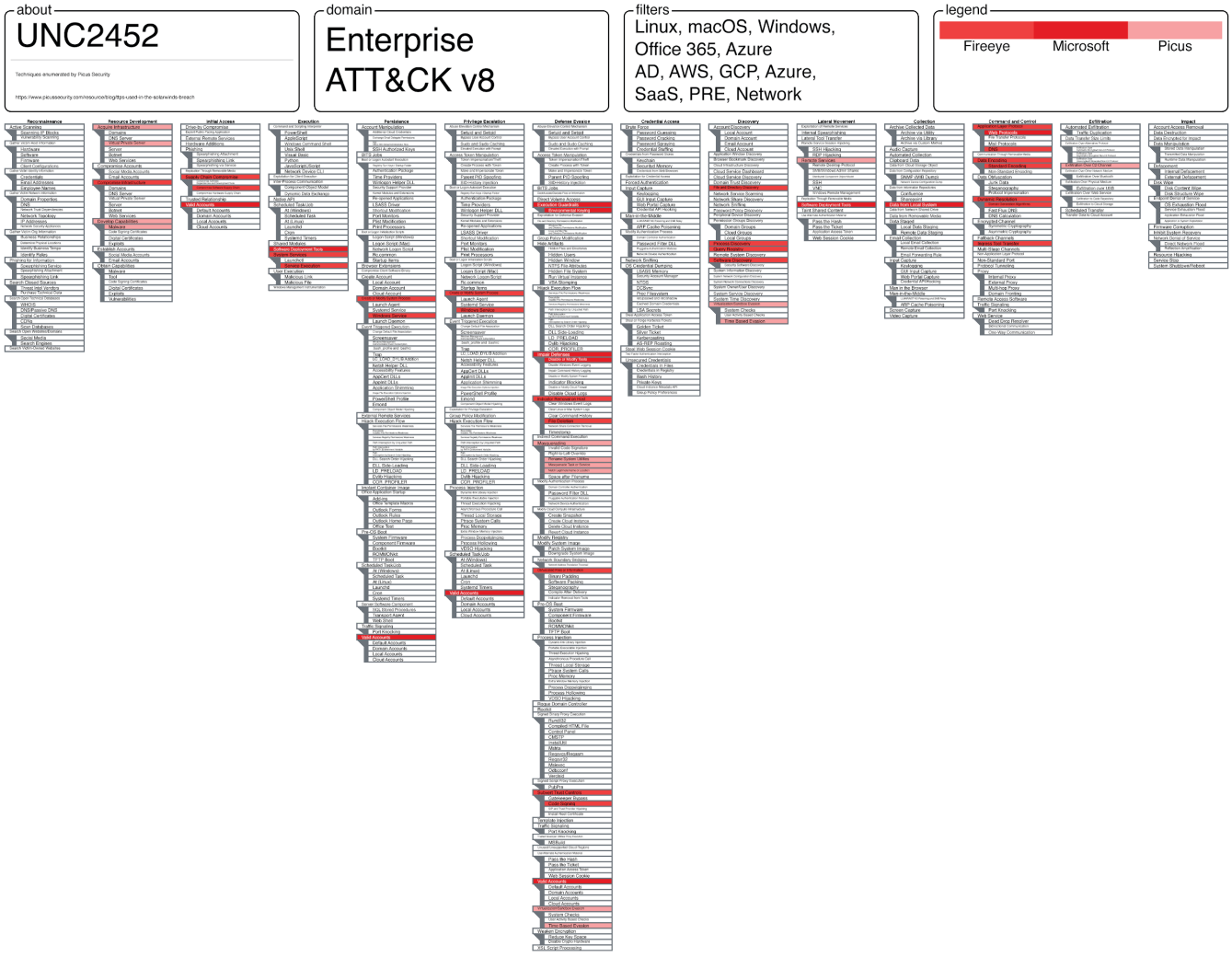
우리의 분석에 따르면, 이 캠페인의 배후에 있는 위협 행위자는 다른 국가 지원 캠페인과 비교해도 대단한 집중력과 끈기를 갖고 있다. 또한 현대의 IT 관행, 아키텍처, 공급망에 대한 고도의 지식을 갖추고 있으며 다양한 공격 기법에 경험이 있다. 그리고 보안 연구원의 기술과 접근방식에도 정통한 것으로 보인다. 하지만 여러 보안 벤더와 업체들이 제공하는 분할된 데이터 수집 등 다양한 요인으로 인해 이 침해에 대한 세부 정보를 완전히 파악할 수는 없다.

SolarWinds 해킹 배후의 위협 행위자는 특정 조직을 겨냥하고 어떤 조직은 의도적으로 배제시킴으로써 타겟을 선택하는 것으로 보인다. 이처럼 신중한 선택은 사이버 범죄 사건에서 흔히 볼 수 있는 기회 표적(Targets of Opportunity)이 아닌, 일련의 요구에 부합되는 표적을 노렸음을 나타낸다. 그럼에도 불구하고 이렇게 엄선된 타겟 가운데 신중한 공격자의 호기심 어린 선택인 FireEye가 포함되었다. 사이버보안 전문업체를 표적으로 삼는 이러한 대담성은 러시아계 해킹 그룹(NotPetya) 과 중국계 해킹 그룹(CCleaner)에서 이전에도 있었다. 이 위협 행위자는 FireEye가 전체 작전을 위험에 빠뜨릴 수 있는 높은 위험을 감수할 만큼 중요한 타겟이라고 생각했거나, 발각되더라도 작전이 실패하지 않을 것이라고 자신했던 것으로 보인다. 혹은 복수심에 이끌렸을 수도 있다. 2016년 힐러리 클린턴 대선 후보 캠프가 해킹당한 것이 국무장관 재직 시절 그녀의 행보 때문이라고 추측하는 사람들도 있다. 어떤 경우이든 이 위협 행위자의 대담함을 보여주며, 이들이 표적에서 제외시킨 기업들의 중요성도 그만큼 커진다. 논리적으로 이들은 공격이 드러날 가능성이 있다고 생각했다면 발각되기까지 시간을 벌기 위해 특정 조직을 타겟에서 제외했을 것이다.

UNC2452에 대한 우리의 분석에서 최종적인 귀결은 없지만, 이것이 우리의 단독 의견은 아니다. 수십여 개 조직에서 사고 대응 및 조사가 진행 중이며, 수백여 곳에서 영향 평가가 이루어지고 있다. 러시아 정보 기관 또는 중국계 해킹 그룹일 것으로 추정하는 이론이 대두되고 있으나 이에 대한 지속적인 검토가 이루어져야 한다. 그러나 우리는 이 캠페인의 배후에 있는 특정 국가가 전술적 방어 행위의 목적과는 무관하다고 결론지었다. 침해 이전에 소요된 작전 시간과 관련 타겟을 놓고 보면 단일 공격자는 필연적으로 풍부한 자금력을 갖춘 국가 지원 세력으로 귀결된다. 캠페인 전체 범위가 명확해지는 대로 향후 수 일, 수 주 이내에 추가 정보가 공개될 것이다. 레코디드 퓨처는 전술적인 측면에서 네트워크 보안을 위해 보안 벤더가 제공하는 조언과 조사 수행을 위한 모범 사례를 따를 것을 권고한다. 전략적인 측면에서는 알려진 기술의 공개 ATT&CK 매트릭스에 단서를 추가할 것을 제안한다. 이러한 방식으로 방어자는 조직의 보안 허점을 파악하고, 영향 수준에 따라 개선 우선순위를 정하고, 조직 전체에 대한 위험을 보다 정확히 평가할 수 있다.

부록

MITRE ATT&CK 분석



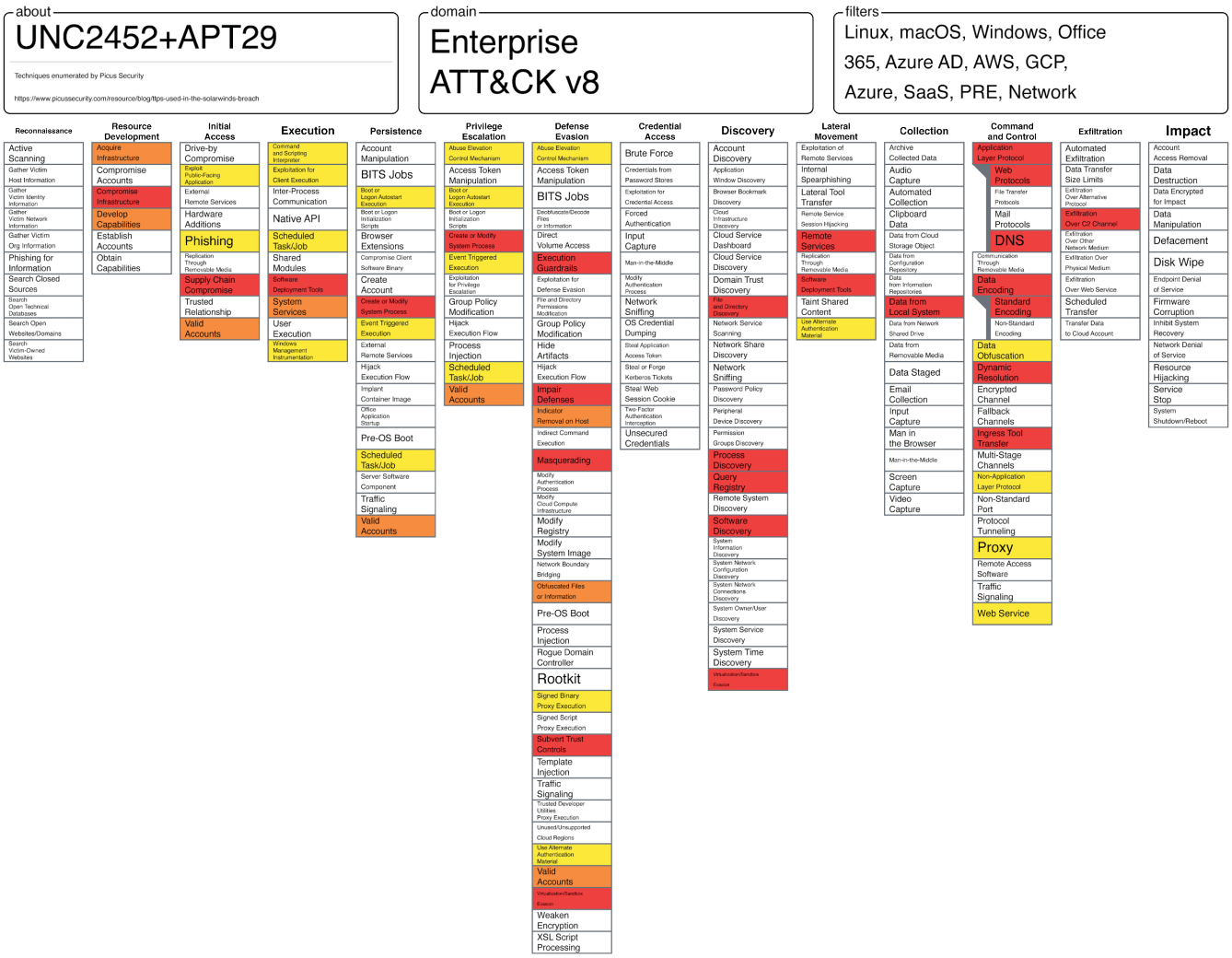
부록 그림 1: ATT&CK Navigator에서 생성된 UNC2452 기술 시각화

우리는 MITRE ATT&CK Enterprise version 8에서 UNC2452의 알려진 기술들을 분석했다. 지금까지 FireEye가 공개한 바에 따르면 MITRE ATT&CK에서 UNC2452는 25가지 공격 기술과 14가지 하위 기술을 가진 것으로 나타난다. (참고: 우리는 UNC2452에 대한 FireEye 보고서에 열거된 기술들과 Picus Security가 취합한 기술들을 비교하였다.) 그런 다음 APT29 및 APT41과 겹치는 UNC2452 기술을 매핑했다. Picus Security는 UNC2452에 대한 분석에 다음과 같은 특정 기술을 추가한다.

- T1021 Remote Services
- T1036.003 Masquerade: Rename System Utilities
- T1036.004 Masquerade Task or Service
- T1036.05 Masquerade: Match Legitimate Name or Location
- T1041 Exfiltration over C2 channel
- T1078 Valid Accounts (also seen in Microsoft report)
- T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion
- T1583.003 Acquire Infrastructure: Virtual Private Servers
- T1587.001 Develop Capabilities: Malware

UNC2452에는 APT29와 동일한 기술이 6가지, APT41과 동일한 기술이 11가지 있다. 9가지 기술은 APT29와 APT41의 알려진 이전 사건에서 볼 수 없었던 새로운 것들이다.

APT29와 기술 비교



부록 그림 2: UNC2452 [빨간색으로 표시]와 APT29 [노란색으로 표시]의 MITRE ATT&CK 매핑. 겹치는 기술은 주황색으로 표시된다.

우리는 FireEye의 UNC2452 관련 보고서를 기반으로 APT29와 겹치는 5가지 기술을 추적했다.

- T1583 Acquire Infrastructure (T1583.003 Private Web Server for UNC2452, T1583.006 Web Server)
- T1587 Develop capabilities, though different sub-techniques (Malware T1587.001 for UNC2452, Digital Certificates T1587.003 for APT29)

Initial Access

- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Execution

- T1569 System Services

Persistence

- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Privilege Escalation
- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Defensive Evasion
- T1070 Indicator Removal on Host (File Deletion T1070.004)
- T1078 Valid accounts (Domain accounts T1078.002 for APT29)
- T1027 Obfuscated Files or Information

상기 내용은 최종적인 정보가 아니지만 중요할 수 있다. APT29에서 확인되었으나 UNC2452 추적에서는 아직 나타나지 않은 기술들은 향후 방어자가 추가로 발견할 수 있는 영역이 될 것이다. 이러한 APT29의 기술이 UNC2452 캠페인에 적용되지 않았을 수도 있고, 반대로 APT29에는 없었지만 UNC2452에서 새롭게 개발된 최신 기술이 사용되었을 수도 있다. 겹치는 부분이 적으면 UNC2452가 APT29와 관련이 없을 가능성도 있으나, 이는 확정적인 것이 아니다. 어느 쪽이든 UNC2452가 궁극적으로 APT29에서 기인했다면, 구조와 기능에 상당한 투자가 있었음을 의미한다.

UNC2452 기술과 APT29 기술의 차이점

UNC2452가 사용하는 특정 기술은 APT29의 알려진 기술 중에서 관찰되지 않았다. 이것은 둘 사이의 연관성을 반증하기 보다는 기술의 확장을 나타낸다고 볼 수 있다. UNC2452가 결국 APT29와 동일하다면 이러한 기술 확장을 지원하는 방대한 리소스가 투입되었다는 결론을 내릴 수 있다.

Initial Access
- T1195 Supply Chain Compromise, Sub-technique T1195.002 Compromise Software Supply Chain

Persistence
- T1543 Create of Modify System Process, Sub-technique T1543.002 Windows Service

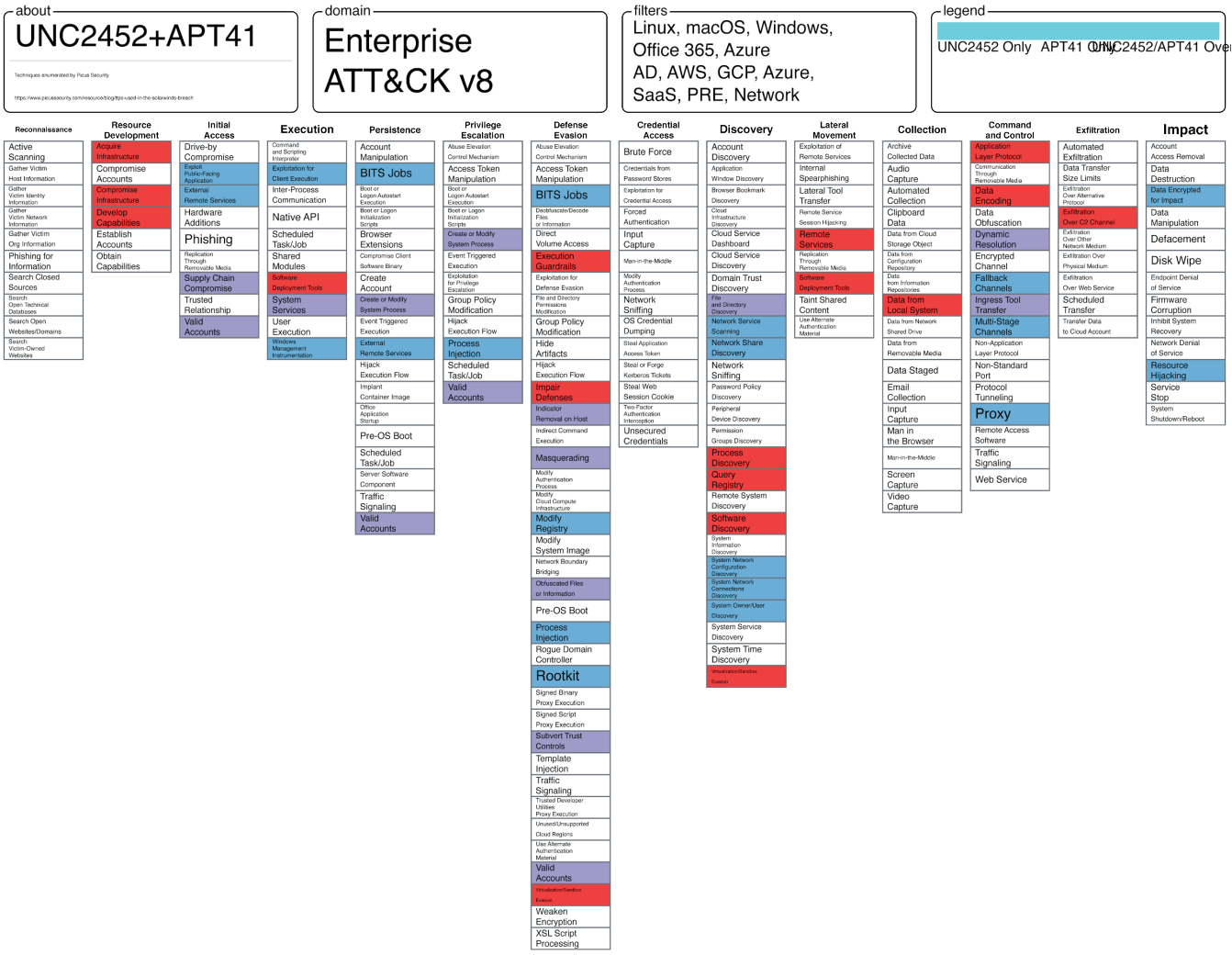
Privilege Escalation
- T1543 Create of Modify System Process, Sub-technique T1543.002 Windows Service

Defensive Evasion
- T1036 Masquerading Sub-techniques T1036.004 Masquerade Task or Service, T1036.05 Match Legitimate Name or Location, T1036.003 Rename System Utilities
- T1553 Subvert Trust Controls, Sub-technique T1553.002 Code Signing
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion

Lateral Movement
- T1021 Remote Services

Command and Control
- T1071 Application Layer Protocol, Sub-technique T1071.001 Web Protocols
- T1568 Dynamic Resolution, T1568.002 Domain Generation Algorithms

APT41과 UNC2452 기술 비교



부록 그림 3: UNC2452와 APT41의 ATT&CK 기술 비교 시각화

일부에서는 APT29 이외의 위협 행위자가 이번 침해의 배후에 있을 가능성을 제기했다. 많이 언급되는 한 가지 가능성은 APT41이다. 미국 법무부는 2020년 9월 국가 관련 스파이 행위와 사이버 범죄 혐의로 7명의 피고인들을 기소하면서 중국을 APT41의 배후로 지적했다. APT41과 UNC2452 간에 중복되는 기술 8개가 확인되었다.

Initial Access

- T1195 Supply Chain Compromise, Sub-technique T1195.002 Compromise Software Supply Chain
- T1078 Valid Accounts

Execution

- T1569 System Services, Sub-technique T1569.002 Service Execution

Persistence

- T1543 Create or Modify System Processes, Sub-technique T1543.003 Windows Service
- T1078 Valid accounts

Privilege Escalation

- T1543 Create or Modify System Processes, Sub-technique T1543.003 Windows Service
- T1078 Valid accounts

Defensive Evasion
- T1070 Indicator Removal on Host, Sub-technique T1070.004 File Deletion
- T1036 Masquerading Sub-techniques T1036.05 Match Legitimate Name or Location
- T1553 Subvert Trust Controls, Sub-technique T1553.002 Code Signing
- T1078 Valid accounts

Command and Control
- T1568 Dynamic Resolution, T1568.002 Domain Generation Algorithms

기타 행위자

이 캠페인의 배후일 가능성이 있는 후보자로 지적된 다른 위협 행위자는 Winnti Group이다. Winnti Group은 CCleaner 공급망 공격에서 확인된 것과 유사한 2019년 DGA 패턴 때문에 후보로 지적되었다. Winnti에 대한 MITRE ATT&CK 그룹 정보는 관련 ATT&CK 기술이 단 3개이므로 추가 분석이 필요하다.

- T1057, Process Discovery, Winnti Group이 감염된 서버에서 실행되는 특정 프로세스 탐색
- T1014, Rootkit , Winnti Group이 루트킷(rootkit)을 사용하여 일반적인 서버 기능 수정
- T1553.002, Subvert Trust Controls: Code Signing, Winnti Group이 훔친 인증서를 사용하여 멀웨어 서명

이러한 기술은 이 캠페인에서 활용된 기술, 특히 사용자들이 신뢰하는 공급망을 활용하는 점과 일치하지만 현재 캠페인은 기술 개발과 피해자 범위 측면에서 훨씬 더 광범위하다.

UNC2452의 새로운 기술

UNC2452의 기술 중 일부는 APT29나 APT41에서 알려진 기술과 전혀 다르다. 또한 이러한 기술은 Winnti에서도 확인되지 않는다. 그러나 이는 적어도 부분적으로 이 행위자에 대한 MITRE ATT&CK 그룹이 불완전한 데 기인한다.

Execution
- T1072 Software Deployment Tools

Defensive Evasion
- T1036 Masquerading, Sub-techniques T1036.004 Masquerade Task or Service, T1036.003 Rename System Utilities
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion

Discovery
- T1057 Process Discovery
- T1012 Query Registry
- T1480.001 Execution Guardrails: Environmental Keying
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion
- T1562.001 Impair Defense: Disable or Modify Tools

Lateral Movement
- T1021 Remote Services

Command and Control
- T1071 Application Layer Protocol, Sub-technique T1071.001 Web Protocols

Exfiltration
- T1041 Exfiltration of C2 Channel

레코디드 퓨처에 대하여

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