랜섬웨어 공격을 통한 북한의 금전 탈취 수법

요 약

참고: 本 사이버 보안 권고문은 미국에서 진행 중인 랜섬웨어 예방 캠페인(#StopRansomware)의 일환으로, 네트워크 방어자들을 위해 다양한 랜섬웨어 변종 및 랜섬웨어 위협 행위자에 대해 상세히 기술하였습니다. 랜섬웨어로부터 모든 기관을 보호하는 노력의 일환으로 발족한 本 랜섬웨어 예방 캠페인 관련 권고문은 현재까지 파악한 TTP와 침해지표를 상세히 설명하고 있습니다. 권고문 全文 및 기타 랜섬웨어 위협 및 무료 지원은 stopransomware.gov 사이트를 참고하시기 바랍니다.

미국 국가안보국(NSA)·연방수사국(FBI)·사이버인프라보안청(CISA)·보건복지부(HHS)와 대한민국 국가정보원·軍 관계기관 DSA(以下 "집필 기관")는 의료·공중 보건 분야 및 기타 주요 인프라 분야 담당 기관에 대한 지속적인 랜섬웨어 활동 관련 경각심을 고취하기 위해 本 합동 사이버 보안 권고문을 발행합니다.

本 보안 권고문은 북한 정권이 지원하는 랜섬웨어에 대한 전반적인 내용과 함께 2022년 7월 6일 발표한 "북한 정권의 지원을 받는 사이버 행위자의 의료 및 공중 보건 분야 대상 Maui 랜섬웨어 사용" 제하의 보고서를 갱신하고자 하며, 랜섬웨어 공격을 목적으로 의료 및 공중 보건 분야와 기타 중요 인프라 분야 기관에 접근하기 위해 북한 사이버 행위자가 사용한 TTP 및 침해지표와 몸값을 요구하기 위해 암호화폐를 사용하는 것에 대한 정보를 담고 있습니다.

집필 기관들은 북한이 암호화폐 활동을 통해 창출한 불특정 수익금을 정권 우선순위 및 정보 목표를 위해 사용한다고 평가하고 있습니다. 이러한 정보 목표는 韓·美 정부와 특히, 국방망 및 방산업체를 대상으로 하는 사이버 활동을 포함합니다. 本 문서의 침해지표는 상기 분야를 포함한 공격 대상 기관에 도움이

될 것으로 사료 됩니다. 한편, 집필 기관은 몸값 지불이 파일과 문서의 복구를 보장하지 않으며 제재 위험을 초래할 수 있음을 말씀드립니다.

북한의 악의적 사이버 활동에 대한 추가 정보는 “북한 사이버 위협 개요 및 권고 사항” 웹페이지를 참고하시기 바랍니다.

기술적 세부 사항

참고: 本 권고문은 기업용 MITRE ATT&CK 프레임워크 version 12를 사용하였습니다. 참조 방법 및 기술에 대해서는 기업용 MITRE ATT&CK을 참고하시기 바랍니다.

本 사이버 보안 권고문은 Maui, H0lyGh0st 랜섬웨어 등 북한의 랜섬웨어 공격을 포함한 악의적 사이버 행위자의 활동에 대한 이전 보고서를 보완하는 차원에서 작성하였으며, 집필 기관들이 추가로 파악한 대한민국과 미국의 의료 시스템 대상 랜섬웨어 공격에 이용된 북한의 TTP를 강조하기 위해 本 권고문을 발행하였습니다.

TTP(전략 · 기술 · 절차) 식별정보

랜섬웨어 공격과 관련된 TTP는, 전통적으로 랜섬웨어 운영에서 관찰되는 TTP 외 인프라 취득 및 구매부터 북한 관련성 은폐까지의 단계로 나눌 수 있습니다.

- **인프라 구축 [T1583].** 북한 해커는 랜섬웨어 공작을 수행하기 위해 도메인, 페르소나, 계정을 생성하고 암호화폐 서비스를 선정합니다. 공격자는 랜섬웨어나 암호화폐 절취 등 불법 사이버 범죄를 통해 획득한 가상자산을 이용해 인프라, IP 주소 및 도메인을 조달합니다.

- **정체 교란.** 북한 해커는 의도적으로 제3의 외국인 협조자를 통해 활동함으로써 북한의 관여를 은폐하고 몸값을 받기 위해 제3의 외국 중개인을 이용합니다.

- **VPN 및 VPS 구매 [T1583.003].** 북한 해커는 또한 가상 사설망(VPN)과 가상 사설 서버(VPS) 및 제3국의 IP 주소를 사용하여 공격이 북한이 아닌 다른 경로에서 온 것처럼 보이게 할 것입니다.

- **접근 권한 획득 [TA0001].** 공격자는 일반적인 취약점을 악용하여 네트워크에 대한 접근 권한과 관리자 권한을 획득합니다. 공격자들이 접근 권한을 얻기 위해 최근 사용한 CVE에는 Apache Log4j 소프트웨어 라이브러리(일명 "Log4Shell")에서의 원격 코드 실행과 다양한 SonicWall 기기에서의 원격 코드 실행[T1190, T1133]이 있습니다. 확인된 CVE는 다음과 같습니다:

  - CVE-2021-44228
  - CVE-2021-20038
  - CVE-2022-24990

공격자는 대한민국의 중소병원 직원이 일반적으로 사용하는 오픈 소스 메신저인 "X-Popup"의 트로이 목마 파일을 통해 악성코드를 퍼뜨릴 가능성이 있습니다 (T1195).

공격자들은 xpopup.pe.kr과 xpopup.com 두 개의 도메인을 활용하여 악성코드를 퍼뜨릴 수 있습니다. xpopup.pe.kr은 IP 주소 115.68.95.128에 할당되어 있었고, xpopup.com은 IP 주소 119.205.197.111에 할당되어 있었습니다. 관련 파일 이름 및 해시는 표 1에 나열되어 있습니다.

표 1: 악성 파일 이름 및 해시 xpopup 도메인을 통해 확산된 악성 파일 이름 및 해시

파일명	MD5
xpopup.rar	1f239db751ce9a374eb9f908c74a31c9
X-PopUp.exe	6fb13b1b4b42bac05a2ba629f04e3d03
X-PopUp.exe	cf8ba073db7f4023af2b13dd75565f3d
xpopup.exe	4e71d52fc39f89204a734b19db1330d3
x-PopUp.exe	43d4994635f72852f719abb604c4a8a1
xpopup.exe	5ae71e8440bf33b46554ce7a7f3de666

- **내부 확산 및 발견 [TA0007, TA0008].** 초기 접근 권한 확보 후, 북한 해커는 맞춤형 악성코드를 포함한 단계별 페이로드를 사용하여 정찰 활동을 수행하고, 추가 파일과 실행 파일을 업로드 및 다운로드하며, 쉘 명령을 실행합니다 [T1083, T1021]. 단계화된 악성코드는 피해자 정보를 수집하여 공격자가 제어하는 원격 호스트로 전송하는 역할도 합니다[TA0010].

- **다양한 랜섬웨어 사용 [TA0040]:** 공격자는 ▲Maui ▲H0lyGh0st 등 자체적으로 개발한 랜섬웨어를 사용해왔습니다[T1486]. 공격자는 암호화를 위해 ▲BitLocker ▲ech0raix ▲GonnaCry ▲Deadbolt ▲Ryuk ▲Hidden Tear ▲Jigsaw ▲My Little Ransomware ▲NxRansomware ▲YourRansom과 같이 공개 도구를 사용하거나 소유하고 있는 것을 확인하였습니다[T1486]. 경우에 따라 북한 해커는 자신을 REvil과 같은 다른 랜섬웨어 조직으로 위장하였습니다. Maui 및 H0lyGh0st 랜섬웨어 사용과 관련된 침해지표는 부록 B를 참조하시기 바랍니다.

- **암호화폐로 몸값 요구:** 북한 해커가 몸값으로 비트코인을 요구하는 것을 파악하였습니다[T1486]. 공격자는 피해자와의 연락을 위해 '프로톤 메일' 계정을 통해 소통하는 것으로 알려져 있습니다. 의료 부문 민간 기업의 경우 공격자는 몸값을 지불하지 않으면 경쟁 업체에 회사 독점 데이터를 노출하겠다고 위협할 수도 있습니다. 북한 해커가 사용할 수 있는 비트코인 지갑 주소는 아래와 같습니다:

- 1MTHBCrBKYEthfa16zo9kabt4f9jMJz8Rm
- bc1q80vc4yjgg6umedkut3e9mhehxl4q4dcjjyzh59
- 1J8spy62o7z2AjQxoUpiCGnBh5cRWKVWJC
- 16ENLdHbnmDcEV8iqN4vuyZHa7sSdYRh76
- bc1q3wzxvu8yhs8h7mlkmf7277wyklkah9k4sm9anu
- bc1q8xyt4jxhw7mgqpwd6qfdjyxgvjeuz57jxrvgk9
- 1NqihEqYaQaWiZkPVdSMiTbt7dTy1LMxgX
- bc1qxrpevck3pq1yzrx2pq2rkvkvy0jnm56nzjv6pw
- 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
- 1KCwfCUgnSy3pzNX7U1i5NwFzRtth4bRBc
- 16sYqXancDDiijcuruZecCkdBDwDf4vSEC
- 1N6JphHFaYmYaokS5xH31Z67bvk4ykd9CP
- LZ1VNJfn6mWjPzkCyoBvqWaBZYXAwn135
- 1KmWW6LgdgykBBrSXrFu9kdoHz95Fe9kQF
- 1FX4W9rrG4F3Uc7gJ18GCwGab8XuW8Ajy2
- bc1qlqgu2l2kms5338zuc95kxavctzyy0v705tpvyc
- bc1qy6su7vrh7ts5ng2628escmhr98msmzg62ez2sp
- bc1q8t69gpxsezdcr8w6tfzp3jeptq4tcp2g9d0mwy
- bc1q9h7yj79sqm4t536q0fdn7n4y2atsvvl22m28ep
- bc1qj6y72rk039mqpgtcy7mwjd3eum6cx6027ndgmd
- bc1qcp557vltuu3qc6pk3ld0ayagrxuf2thp3pjzpe
- bc1ql8wsflrjf9zlusauynzjm83mupq6c9jz9vnqxg
- bc1qx60ec3nfd5yhsyyxkzkpts54w970yxj84zrdck
- bc1qunqnjdlvqkjuhtclfp8kzkjpvdz9qnk898xczp
- bc1q6024d73h48fnhwswhwt3hqz2lzw6x99q0nulm4
- bc1qwdvexlyvg3mqvqw7g6l09qup0qew80wjj9jh7x
- bc1qavrtge4p7dmcrnvhlvuhaarx8rek76wxyk7dgg
- bc1qagaayd57vr25dlqgk7f00nhz9qepqgnlnt4upu
- bc1quvnaxnpqlzq3mdhfddh35j7e7ufxh3gpc56hca

- bc1qu0pvfmtxawm8s99lcjvxapungtsmkvwyvak6cs
- bc1qg3zlxxhhcvt6hkuhmqml8y9pas76cajcu9ltdl
- bc1qn7a3g23nzpuytchyyteyhkcse84cnylznl3j32
- bc1qhfmqstxp3yp9muvuz29wk77vjtdyrkff4nrxpu
- bc1qnh8scrvuqvlzmzgw7eesyrmtes9c5m78duetf3
- bc1q7qry3lsrphmnw3exs7tkwzpvzjcxs942aq8n0y
- bc1qcmlcxfsy0zlqhh72jvvc4rh7hvwhx6scp27na0
- bc1q498fn0gauj2kkjsg35mlwk2cnxhaqlj7hkh8xy
- bc1qnz4udqkumjghnm2a3zt0w3ep8fwdcyv3krr3jq
- bc1qk0saaw7p0wrwla6u7tfjlxrutlgrwnudzx9tyw
- bc1qyue2pgjk09ps7qvfs559k8kee3jkcw4p4vdp57
- bc1q6qfkt06xmrpclht3acmq00p7zyy0ejydu89zwv
- bc1qmge6a7sp659exnx78zhm9zgrw88n6un0rl9trs
- bc1qcywkd7zqlwmjy36c46dpf8cq6ts6wgkjx0u7cn

예방 대책

집필 기관들은 의료 및 공중 보건 기관들에 대해 다음을 촉구합니다:

- 네트워크, IoT 의료 기기 및 전자 건강 기록 시스템과의 연결을 인증하고 전송 중에 데이터 패키지가 조작되지 않도록 공개 키 인프라와 디지털 인증서를 도입하여 데이터에 대한 접근을 제한하시기 바랍니다.
- 과도한 시스템 관리 권한 부여 및 최소한의 권한 보장을 하지 않는 관리자 계정 대신 내부 시스템에서 표준 사용자 계정을 사용하시기 바랍니다.
- WAN(광역 네트워크)의 경우, Telnet, SSH, Winbox 및 HTTP와 같은 네트워크 장치 관리 인터페이스를 끄고, 활성화된 경우 강력한 패스워드 및 암호화로 보호하시기 바랍니다.
- 개인 식별 가능 정보와 민감한 건강 정보는 수집 지점에서부터 보호하고, TLS(전송 계층 보안)와 같은 기술을 사용하여 미사용 데이터와 전송 중인 데이터를 암호화하시기 바랍니다. 개인 환자 데이터는 방화벽으로 보호되는

내부 시스템에만 저장하고 데이터가 손상된 경우에도 전체적인 백업을 사용할 수 있도록 합니다.

- 영구 계정 번호를 표시할 때는 마스킹하고 저장할 때는 암호화 등을 통해 읽을 수 없도록 렌더링하여 저장된 데이터를 보호하시기 바랍니다.
- 1996년 제정된 건강보험 이전과 책임에 관한 법(HIPAA)과 같은 규정에 따라 개인 식별 정보와 민감 건강 정보에 대한 수집·저장 및 처리 관행을 보호합니다. HIPAA 보안 조치를 구현하면 시스템에 악성 프로그램이 유입되는 것을 방지할 수 있습니다.
- '다중 계층 네트워크 세분화'를 구현하여 가장 중요한 통신 및 데이터는 가장 안전하고 신뢰할 수 있는 계층에 저장하시기 바랍니다.
- 모니터링 도구를 사용하여 침해로 인해 IoT 장비가 비정상적으로 작동하는지 관찰하시기 바랍니다.
- 개인 식별 정보와 민감 건강 정보의 수집·저장·접근 및 모니터링을 규제하는 내부 정책을 수립하고 정기적으로 검토합니다.

또한, 집필 기관은 의료 및 공중 보건 분야 조직을 포함한 모든 조직이 랜섬웨어 사고에 대비하고 피해를 줄이기 위해 다음 권장 사항을 적용할 것을 촉구합니다.

- **데이터의 오프라인 (즉, 물리적 연결 해제) 백업을 유지하고 정기적으로 백업 및 복원을 테스트합니다.** 이러한 훈련은 조직의 운영 지속성을 보호하며 적어도 랜섬웨어 사고로 인한 가동 중지 시간을 최소화하고 데이터 손실을 방지할 수 있습니다.
  - 모든 백업 데이터가 암호화되고 변경 불가능하며 전체 조직의 데이터 인프라를 포함하는지 확인합니다.
- 랜섬웨어 사고에 대한 대응 절차를 포함하는 **기본 사이버 사고 대응 계획 및 관련 커뮤니케이션 계획을 수립하고 실행합니다.**
  - 사고 대응 계획 및 커뮤니케이션 계획에 데이터 침해 사고 대응 및 알림

절차를 포함하도록 합니다. 통지 절차가 관련 법률을 준수하는지 확인하시기 바랍니다.

- 랜섬웨어 대응 체크리스트 작성 및 랜섬웨어로 인한 데이터 유출 계획 수립·대응에 관한 내용은 CISA와 MS-ISAC 합동 랜섬웨어 가이드 및 CISA의 "랜섬웨어로 인한 데이터 유출로부터 민감하고 개인적인 정보 보호" 팩트 시트를 참조하시기 바랍니다.

• **OS, 소프트웨어 및 펌웨어 업데이트가 출시되는 즉시 설치하시기 바랍니다.** 시기적절한 패치는 조직이 사이버 보안 위협에 대한 노출을 최소화하기 위해 취할 수 있는 가장 효율적이고 경제적인 방법의 하나입니다. 정기적으로 소프트웨어 업데이트 및 지원 종료 알림을 확인하고, 악용된 것으로 알려진 취약점 패치를 우선 적용합니다. 프로세스를 자동화하고 신속하게 처리하기 위해 중앙 집중식 패치 관리 시스템을 활용하는 방안을 고려해보시기 바랍니다.

• **원격 데스크톱 프로토콜 또는 기타 잠재적으로 위험한 서비스를 사용하는 경우 이를 보호하고 면밀히 모니터링하십시오.**

- RDP를 제한하고 가상 데스크톱 인프라를 사용하여 내부망을 통해 내부 자산에 접근하는 것을 예방하시기 바랍니다. 위험 평가 후 지속적으로 RDP가 운영상 필요하다고 판단하는 경우, 접근 원점을 제한하고 자격증명 도용 및 재사용을 최소화하기 위해 피싱을 방지하는 다단계 인증을 도입하시기 바랍니다. RDP를 외부에서 사용해야 하는 경우, RDP가 내부 장치에 접속하도록 허용하기 전에 VPN이나 가상 데스크톱 인프라 또는 기타 방법을 이용하여 접속을 인증하고 보호하시기 바랍니다. ▲원격 접속 로그를 모니터링하고 ▲무차별 대입 공격을 차단하기 위해 지정된 횟수만큼 시도한 후 계정 잠금을 시행하며 ▲RDP 로그인 시도를 기록하고 ▲사용하지 않는 원격 접속 포트는 비활성화하시기 바랍니다.

- 장치가 제대로 구현되어 있고 보안 기능이 활성화되어 있는지 확인하시기 바랍니다. 예를 들어, RDP 전송 제어 프로토콜 포트인 3389와 같이 비즈니스 목적으로 사용되지 않는 포트 및 프로토콜을 비활성화합니다.

- 네트워크 內 SMB(서버 메시지 블록) 프로토콜은 필요한 서버에만 접근할 수 있도록 제한하고, SMB 버전 1 등 SMB의 오래된 버전을 제거하거나 비활성화 합니다. 공격자는 SMB를 사용하여 조직 전체에 악성코드를 전파합니다.
- 타사 공급업체 및 귀사와 상호 연결된 공급업체의 보안 상태를 점검합니다. 타사 공급업체와 외부 소프트웨어·하드웨어 간의 모든 연결을 모니터링 하고 의심스러운 활동이 있는지 검토하시기 바랍니다.
- 상용화되고 승인된 프로그램만 시스템이 실행하도록 허용하는 어플리케이션 제어 정책을 구현하시기 바랍니다.
- 활성 콘텐츠가 실행되지 않도록 보호된 '보기 모드'에서 문서 뷰어를 실행 하시기 바랍니다.

- 웹 사이트 방문, 링크 클릭 및 첨부 파일 열기의 위험에 대한 사용자의 인식을 높이기 위해 **사용자 교육 프로그램 및 피싱 훈련을 시행하시기 바랍니다.**
- **최대한 많은 서비스에 대해 피싱 방지를 위한 다중 인증이 필요합니다.** 특히, 웹 메일, VPN, 중요 시스템에 접속하는 계정 및 백업 관리 권한 계정의 경우 다중 인증을 필수적으로 하시기 바랍니다.
- **강력한 암호를 사용**하고 여러 계정에 암호를 재사용하지 마십시오. 자세한 내용은 CISA의 "비밀번호 선택 및 보호" 조언 및 미국표준기술연구소의 "특별 간행물 800-63B: 디지털 ID 가이드라인" 문서를 참조하시기 바랍니다.
- **소프트웨어를 설치하려면 관리자 자격증명을 요구합니다.**
- **관리자 권한 및 권한 상승을 통해 사용자 계정을 점검하고**, 최소한의 권한으로 접근 제어를 구성하시기 바랍니다.
- **모든 호스트에 바이러스 백신 및 악성코드 방지 소프트웨어를 설치하고 정기적으로 업데이트합니다.**
- **보안 네트워크만을 사용하고 공용 Wi-Fi 네트워크는 사용하지 않습니다.** VPN 설치 및 사용을 고려하시기 바랍니다.

- **조직 외부에서 오는 메시지에** 위험도가 더 높은 메시지임을 나타내는 **이메일 배너를 추가하는 것을 고려하시기 바랍니다.**
- **수신한 이메일에서 하이퍼링크를 비활성화합니다.**
- 기계가 이해할 수 있는 사이버 위협 지표와 방어 조치를 실시간으로 공유하기 위해 **CISA의 AIS(자동 지표 공유) 참여를 고려해봅니다.** AIS는 공공 및 민간 부문 파트너와 협력하여 정보 공유를 통해 사이버 위협을 식별 및 완화하고 요청 시 사고를 예방·탐지 및 대응하는 데 도움이 되는 기술 지원을 제공하는 CISA 임무의 일환이며, 무료로 제공됩니다.

貴社에서 랜섬웨어 사고가 발생한 경우:

- 貴社의 랜섬웨어 대응 체크리스트를 따릅니다.
- 백업을 검사합니다. 가능한 경우, 바이러스 백신 프로그램으로 백업 데이터를 검사하여 악성코드가 없는지 확인합니다.
- **미국 기관**: 사이버 사고 대응 계획에 명시한 알림 요구 사항을 준수하고, FBI(연방수사국), CISA(사이버인프라보안청) 또는 USSS(미국비밀임무국) 등 관련 당국에 사건을 보고합니다.
- **대한민국 기관**: 국가정보원, 한국인터넷진흥원 또는 경찰청에 사고를 신고하십시오.
  - 국가정보원
    · 전화번호 : 111
    · https://www.nis.go.kr
  - 한국인터넷진흥원
    · 전화번호 : 118 (상담 서비스)
    · https://www.boho.or.kr/consult/ransomware.do
  - 경찰청
    · 사이버범죄 신고시스템:
    https://ecrm.police.go.kr/minwon/main

- CISA와 濠・加・뉴질랜드・英 사이버보안 당국이 공동으로 작성한 “악의적인 활동 탐지 및 해결을 위한 기술적 접근 방식” 제하의 사이버보안 권고문에 수록된 사고 대응 모범 사례를 적용합니다.

참 고

Stairwell社는 다음 링크에서 Maui 랜섬웨어를 식별하는 YARA 규칙과 RSA Public 키 추출기의 개념 증명을 제공합니다:
https://www.stairwell.com/news/threat-research-report-maui-ransomware/

요청 사항

FBI는 외부 IP 주소와의 통신을 보여주는 로그, 비트코인 지갑 정보, 암호 해독기 파일 및/또는 암호화된 파일의 샘플을 포함 공유 가능한 모든 정보를 수집하고 있습니다. 위에서 언급한 바와 같이, 집필 기관은 몸값을 지불하는 것을 권장하지 않습니다. 몸값 지불은 파일 복구를 절대 보장하지 않으며, 다른 기관을 추가적인 공격목표로 삼도록 하고, 다른 범죄 행위자가 랜섬웨어 유포에 관여하거나 불법 활동에 자금을 대도록 장려할 수 있습니다. 하지만 피해자가 손쓸 수 없는 상황에 직면했을 때 주주, 직원과 고객을 보호하기 위해 모든 옵션을 고려할 수밖에 없다는 사실을 충분히 이해합니다.

귀하 또는 귀하의 기관이 몸값을 지불하기로 했는지에 관계없이, 상기 연락처 정보를 통해 랜섬웨어 사건을 즉시 신고하여주시기 바랍니다.

감사의 말

미국 국가안보국(NSA)・사이버인프라보안청(CISA)・연방수사국(FBI) 및 보건복지부(HHS)는 本 보안 권고문에 대한 기여와 파트너십에 대해 대한민국 국가정보원과 DSA에 감사드립니다.

보증의 면책

本 문서상 상호, 상표, 제조업체 또는 기타 방법을 통해 특정 상업용 제품이나 프로세스 또는 서비스를 언급하였다고 하더라도 미국 정부의 승인·권장 및 선호를 나타내는 것은 아니며, 本 지침은 광고나 제품 보증 목적으로 사용되어서는 안 됩니다.

상표 인식

Microsoft Threat Intelligence Center는 Microsoft Corporation의 등록 상표입니다. Apache®, Sonicwall 및 Apache Log4j는 Apache Software Foundation의 상표입니다. TeraMaster 운영 체제는 Octagon Systems의 등록 상표입니다.

목 적

本 문서는 위협을 파악 및 전파하고 사이버 보안 사양 및 해결방안을 개발 및 발행하는 책임을 포함하여 저자의 사이버 보안 임무를 강화하기 위해 개발되었습니다. 모든 이해관계자의 인식 제고를 위해 이 정보를 광범위하게 공유할 수 있습니다.

부록 A: 취약점 세부 정보

CVE-2021-44228	CVSS 3.0: 10 (심각)
취약점 설명 Apache Log4j2 2.0-bet9부터 2.15.0(보안 릴리즈 2.12.2, 2.12.3 및 2.3.1 제외)의 JNDI 기능은 공격자가 제어하는 LDAP 및 기타 JNDI 관련 엔드포인트에 대해 보호하지 않습니다. 로그 메시지 또는 로그 메시지 매개 변수를 제어할 수 있는 공격자는 '메시지 조회 대체'가 활성화된 경우 LDAP 서버에서 로드된 임의 코드를 실행할 수 있습니다. Log4j 2.15.0부터는 이 동작이 기본적으로 비활성화되었습니다. 버전 2.16.0(2.12.2, 2.12.3 및 2.3.1과 함께)에서 이 기능은 완전히 제거되었습니다. 이 취약점은 log4j-core에만 해당하며 log4net, log4cxx 또는 기타 Apache Logging Services 프로젝트에는 영향을 미치지 않습니다.	
권장하는 예방 대책 공급업체에서 제공하는 패치를 적용하고 필요한 시스템 업데이트를 수행하십시오.	
탐지 방안 Log4j 2 취약점의 악용 방지, 감지 및 추적에 대한 공급업체의 지침을 참조하십시오.	
취약한 기술 및 버전 CVE-2021-44228과 관련된 수많은 취약한 기술 및 버전이 있습니다. 전체 목록은 https://nvd.nist.gov/vul에서 확인하십시오.	
자세한 내용은 https://nvd.nist.gov/vuln/detail/CVE-2021-44228을 참조하십시오.	

CVE-2021-20038	CVSS 3.0: 9.8 (심각)

취약점 설명

SMA100 Apache httpd 서버의 mod_cgi 모듈 환경 변수에 있는 스택 기반 버퍼 오버플로 취약성으로 인해 인증되지 않은 원격 공격자가 어플라이언스에서 'nobody' 사용자로 코드를 실행할 수 있습니다. 이 취약점은 SMA 200, 210, 400, 410 및 500v 어플라이언스 펌웨어 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv 및 이전 버전에 영향을 미쳤습니다.

권장하는 예방 대책

모든 적절한 공급업체 업데이트를 적용하십시오.

업그레이드:

- SMA 100 시리즈 - SMA 200, 210, 400, 410, 500v (ESX, Hyper-V, KVM, AWS, Azure)
- SonicWall SMA100 빌드 버전 10.2.0.9-41sv 이상
- SonicWall SMA100 빌드 버전 10.2.0.9-41sv 이상

시스템 관리자는 영향을 받는 어플리케이션 · 시스템 및 적절한 수정 조치를 결정하기 위해 참조 섹션의 SonicWall 보안 권고문을 참고해야 합니다.

9.0.0 펌웨어에 대한 지원이 2021년 10월 31일에 종료되었습니다. 해당 펌웨어를 계속 사용하는 고객은 최신 10.2.x 버전으로 업그레이드해야 합니다.

취약한 기술 및 버전

Sonicwall Sma 200 Firmware 10.2.0.8-37Sv
Sonicwall Sma 200 Firmware 10.2.1.1-19Sv
Sonicwall Sma 200 Firmware 10.2.1.2-24Sv
Sonicwall Sma 210 Firmware 10.2.0.8-37Sv
Sonicwall Sma 210 Firmware 10.2.1.1-19Sv
Sonicwall Sma 210 Firmware 10.2.1.2-24Sv
Sonicwall Sma 410 Firmware 10.2.0.8-37Sv
Sonicwall Sma 410 Firmware 10.2.1.1-19Sv
Sonicwall Sma 410 Firmware 10.2.1.2-24Sv
Sonicwall Sma 400 Firmware 10.2.0.8-37Sv
Sonicwall Sma 400 Firmware 10.2.1.1-19Sv
Sonicwall Sma 400 Firmware 10.2.1.2-24Sv
Sonicwall Sma 500V Firmware 10.2.0.8-37Sv
Sonicwall Sma 500V Firmware 10.2.1.1-19Sv
Sonicwall Sma 500V Firmware 10.2.1.2-24Sv

자세한 내용은 https://nvd.nist.gov/vuln/detail/CVE-2021-20038을 참조하십시오.

CVE-2022-24990	CVSS 3.x: 해당 없음
취약점 설명 PHP 객체 인스턴스화 취약점을 통한 TerraMaster OS에서의 인증되지 않은 원격 명령 실행 취약점은 원격 공격자가 대상 엔드포인트에서 명령을 실행할 수 있도록 하는 스크립트의 결함을 대상으로 하는 스캔 활동을 특징으로 합니다. 이 취약점은 api.php 스크립트에서 webNasIPS 구성 요소의 부적절한 입력 유효성 검사로 인해 생성되며, 사용자가 스토리지를 관리하고 데이터를 백업하고 어플리케이션을 구성하는 TNAS 장치 어플라이언스의 운영 체제에 상주합니다. 인증되지 않은 원격 공격자는 이 스크립트 결함을 악용하여 특별히 제작된 데이터를 어플리케이션에 전달하고 대상 시스템에서 임의의 명령을 실행할 수 있습니다. 이로 인해 정보 유출을 포함하여 대상 시스템이 완전히 손상될 수 있습니다. TNAS 장치는 인증되지 않은 원격 코드 실행을 획득하기 위해 가장 높은 권한으로 연결될 수 있습니다.	
권장하는 예방 대책 관련 공급업체 패치를 설치하십시오. 이 취약점은 TOS 버전 4.2.30에서 패치되었습니다.	
취약한 기술 및 버전 TOS v 4.2.29	
자세한 내용은 https://octagon.net/blog/2022/03/07/cve-2022-24990-terrmaster-tos-unauthenticated-remote-command-execution-via-php-object-instantiation/을 참조하십시오.	

부록 B: 침해지표

침해지표 섹션에는 Maui 및 H0lyGh0st 랜섬웨어 변종과 함께, 북한 사이버 공격자가 개발한 것으로 추정하는 원격 제어 트로이 목마, 로더 및 랜섬웨어 후속 배포를 가능하게 하는 기타 도구 등 맞춤형 악성코드에 대한 해시 및 IP 주소를 포함하고 있습니다. Maui 침해지표에 대한 추가 정보는 "북한 정부의 지원을 받는 사이버 행위자들이 의료 및 공중 보건 분야를 대상으로 Maui 랜섬웨어를 사용" 합동 사이버 보안 권고문을 참조하시기 바랍니다.

표 2에는 북한 사이버 행위자들이 사용하는 악성코드, 백도어 및 Maui 랜섬웨어 파일의 드롭퍼를 포함한 기타 도구들과 관련된 MD5 및 SHA256 해시를 포함합니다.

표 2: 악성코드, 백도어 및 도구의 파일 이름 및 해시

MD5	SHA256
079b4588eaa99a1e802adf5e0b26d8aa	f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7
0e9e256d8173854a7bc26982b1dde783	--
12c15a477e1a96120c09a860c9d479b3	6263e421e397db821669420489d2d3084f408671524fd4e1e23165a16dda2225
131fc4375971af391b459de33f81c253	--
17c46ed7b80c2e4dbea6d0e88ea0827c	b9af4660da00c7fa975910d0a19fda072031c15fad1eef935a609842c51b7f7d
1875f6a68f70bee316c8a6eda9ebf8de	672ec8899b8ee513dbfc4590440a61023846ddc2ca94c88ae637144305c497e7
1a74c8d8b74ca2411c1d3d22373a6769	ba8f9e7afe5f78494c111971c39a89111ef9262bf23e8a764c6f65c818837a44
1f6d9f8fbdbbd4e6ed8cd73b9e95a928	4f089afa51fd0c1b2a39cc11cedb3a4a326111837a5408379384be6fe846e016
2d02f5499d35a8dffb4c8bc0b7fec5c2	830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
2e18350194e59bc6a2a3f6d59da11bd8	655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae

MD5	SHA256
3bd22e0ac965ebb6a18bb71ba39e96dc	6b7f566889b80d1dba4f92d5e2fb2f5ef2 4f57fcfd56bb594978dffe9edbb9eb
40f21743f9cb927b2c84ecdb7dfb14a6	5081f54761947bc9ce4aa2a259a0bd60b4 ec03d32605f8e3635c4d4edaf48894
4118d9adce7350c3eedeb056a3335346	5b7ecf7e9d0715f1122baf4ce745c5fcd7 69dee48150616753fec4d6da16e99e
43e756d80225bdf1200bc34eef5adca8	afb2d4d88f59e528f0e388705113ae54b7 b97db4f03a35ae43cc386a48f263a0
47791bf9e017e3001ddc68a7351ca2d6	863b707873f7d653911e46885e261380b4 10bb3bf6b158daefb47562e93cb657
505262547f8879249794fc31eea41fc6	f32f6b229913d68daad937cc72a57aa452 91a9d623109ed48938815aa7b6005c
5130888a0ad3d64ad33c65de696d3fa2	c92c1f3e77a1876086ce530e87aa9c1f9c bc5e93c5e755b29cad10a2f3991435
58ad3103295afcc22bde8d81e77c282f	18b75949e03f8dcad513426f1f9f3ca209 d779c24cd4e941d935633b1bec00cb
5be1e382cd9730fbe386b69bd8045ee7	5ad106e333de056eac78403b033b89c58b 4c4bdda12e2f774625d47ccfd3d3ae
5c6f9c83426c6d33ff2d4e72c039b747	a3b7e88d998078cfd8cdf37fa5454c45f6 cbd65f4595fb94b2e9c85fe767ad47
640e70b0230dc026eff922fb1e44c2ea	6319102bac226dfc117c3c9e620cd99c7e afbf3874832f2ce085850aa042f19c
67f4dad1a94ed8a47283c2c0c05a7594	3fe624c33790b409421f4fa2bb8abfd701 df2231a959493c33187ed34bec0ae7
70652edadedbacfd30d33a826853467d	196fb1b6eff4e7a049cea323459cfd6c0e 3900d8d69e1d80bffbaabd24c06eba
739812e2ae1327a94e441719b885bd19	6122c94cbfa11311bea7129ecd5aea6fae 6c51d23228f7378b5f6b2398728f67
76c3d2092737d964dfd627f1ced0af80	bffe910904efd1f69544daa9b72f2a70fb 29f73c51070bde4ea563de862ce4b1
802e7d6e80d7a60e17f9ffbd62fcbbeb	87bdb1de1dd6b0b75879d8b8aef80b562e c4fad365d7abbc629bcfc1d386afa6
827103a6b6185191fd5618b7e82da292	--
830bc975a04ab0f62bfedf27f7aca673	--

MD5	SHA256
85995257ac07ae5a6b4a86758a2283d7	--
85f6e3e3f0bdd0c1b3084fc86ee59d19	f1576627e8130e6d5fde0dbe3dffcc8bc9eef1203d15fcf09cd877ced1ccc72a
87a6bda486554ab16c82bdfb12452e8b	980bb08ef3e8afcb8c0c1a879ec11c41b29fd30ac65436495e69de79c555b2be
891db50188a90ddacfaf7567d2d0355d	0837dd54268c373069fc5c1628c6e3d75eb99c3b3efc94c45b73e2cf9a6f3207
894de380a249e677be2acb8fbdfba2ef	--
8b395cc6ecdec0900facf6e93ec48fbb	--
92a6c017830cda80133bf97eb77d3292	d1aba3f95f11fc6e5fec7694d188919555b7ff097500e811ff4a5319f8f230be
9b0e7c460a80f740d455a7521f0eada1	45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
9b9d4cb1f681f19417e541178d8c75d7	f5f6e538001803b0aa008422caf2c3c2a79b2eeee9ddc7feda710e4aba96fea4
a1f9e9f5061313325a275d448d4ddd59	dfdd72c9ce1212f9d9455e2bca5a327c88d2d424ea5c086725897c83afc3d42d
a452a5f693036320b580d28ee55ae2a3	99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f
a6e1efd70a077be032f052bb75544358	3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878
ad4eababfe125110299e5a24be84472e	a557a0c67b5baa7cf64bd4d42103d3b2852f67acf96b4c5f14992c1289b55eaa
b1c1d28dc7da1d58abab73fa98f60a83	38491f48d0cbaab7305b5ddca64ba41a2beb89d81d5fb920e67d0c7334c89131
b6f91a965b8404d1a276e43e61319931	--
bdece9758bf34fcad9cba1394519019b	9d6de05f9a3e62044ad9ae66111308ccb9ed2ee46a3ea37d85afa92e314e7127
c3850f4cc12717c2b54753f8ca5d5e0e	99b448e91669b92c2cc3417a4d9711209509274dab5d7582baacfab5028a818c
c50b839f2fc3ce5a385b9ae1c05def3a	458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456
cf236bf5b41d26967b1ce04ebbdb4041	60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145

MD5	SHA256
d0e203e8845bf282475a8f816340f2e8	f6375c5276d1178a2a0fe1a16c5668ce523e2f846c073bf75bb2558fdec06531
ddb1f970371fa32faae61fc5b8423d4b	dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
f2f787868a3064407d79173ac5fc0864	92adc5ea29491d9245876ba0b2957393633c9998eb47b3ae1344c13a44cd59ae
fda3a19afa85912f6dc8452675245d6b	56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19
--	0054147db54544d77a9efd9baf5ec96a80b430e170d6e7c22fcf75261e9a3a71
--	151ab3e05a23e9ccd03a6c49830dabb9e9281faf279c31ae40b13e6971dd2fb8
--	1c926fb3bd99f4a586ed476e4683163892f3958581bf8c24235cd2a415513b7f
--	1f8dcfaebbcd7e71c2872e0ba2fc6db81d651cf654a21d33c78eae6662e62392
--	f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
--	23eff00dde0ee27dabad28c1f4ffb8b09e876f1e1a77c1e6fb735ab517d79b76
--	586f30907c3849c363145bfdcdabe3e2e4688cbd5688ff968e984b201b474730
--	8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
--	90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
--	c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
--	ca932ccaa30955f2fffb1122234fb1524f7de3a8e0044de1ed4fe05cab8702a5
--	f6827dc5af661fbb4bf64bc625c78283ef836c6985bb2bfb836bd0c8d5397332
--	f78cabf7a0e7ed3ef2d1c976c1486281f56a6503354b87219b466f2f7a0b65c4

표 3에는 Maui 랜섬웨어 파일들과 관련된 MD5 및 SHA256 해시를 포함합니다.

표 3: Maui 랜섬웨어 파일의 파일 이름 및 해시

MD5	SHA256
4118d9adce7350c3eedeb056a3335346	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e
9b0e7c460a80f740d455a7521f0eada1	45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
fda3a19afa85912f6dc8452675245d6b	56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19
2d02f5499d35a8dffb4c8bc0b7fec5c2	830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
c50b839f2fc3ce5a385b9ae1c05def3a	458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456
a452a5f693036320b580d28ee55ae2a3	99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f
a6e1efd70a077be032f052bb75544358	3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878
802e7d6e80d7a60e17f9ffbd62fcbbeb	87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6
--	0054147db54544d77a9efd9baf5ec96a80b430e170d6e7c22fcf75261e9a3a71

표 4에는 H0lyGh0st 랜섬웨어 파일들과 관련된 MD5 및 SHA256 해시를 포함합니다.

표 4: H0lyGh0st 랜섬웨어 파일의 파일 이름 및 해시

SHA256
99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd*
F8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86*
Bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af*
6e20b73a6057f8ff75c49e1b7aef08abfcfe4e418e2c1307791036f081335c2d
f4d10b08d7dacd8fe33a6b54a0416eecdaed92c69c933c4a5d3700b8f5100fad
541825cb652606c2ea12fd25a842a8b3456d025841c3a7f563655ef77bb67219
2d978df8df0cf33830aba16c6322198e5889c67d49b40b1cb1eb236bd366826d

414ed95d14964477bebf86dced0306714c497cde14dede67b0c1425ce451d3d7
Df0c7bb88e3c67d849d78d13cee30671b39b300e0cda5550280350775d5762d8
MD5
a2c2099d503fcc29478205f5aef0283b
9c516e5b95a7e416gecbd133ed4d205f
d6a7b5db62bf7815a10a17cdf7ddbd4b
c6949a99c60ef29d20ac8a9a3fb58ce5
4b20641c75ged563757cdd95c651ee53
25ee4001eb4e91f7ea0bc5d07f2a9744
29b6b54e10a96e6c40e1f0236b01b2e8
18126be163eb7df2194bb902c359ba8e
eaf6896b361121b2c315a35be837576d
e4ee611533a28648a350f2dab85bb72a
e268cb7ab778564e88d757db4152b9fa

* H0lyGh0st에 대한 마이크로소프트 블로그 게시물에서 발췌