サイバーセキュリティレポート

2023.10

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

© NTT Security Holdings

目次

【1 ページサマリー】 3
1. ハクティビストグループがランサムウェア GhostLocker を発表 4
1.1. 概要 4
1.2. The Five Families の結成 4
1.3. ランサムウェア「GhostLocker」 7
1.4. まとめ 8
2. Cisco の IOS XE にゼロデイ脆弱性、4 万台以上に不正プログラムが設置される 9
2.1. 概要 9
2.2. IOS XE と脆弱性について 9
2.3. 管理インターフェイスを公開するリスク 11
2.4. まとめ 11
3. パレスチナにおける武力衝突とサイバー攻撃 12
3.1. 概要 12
3.2. 勃発直後から発生したサイバー戦 12
3.3. 重要インフラを狙うハクティビストの活動 13
3.4. 赤十字国際委員会（ICRC）が提案するサイバー攻撃のルール 14
3.5. まとめ 15

© NTT Security Holdings

【1 ページサマリー】

当レポートでは 2023 年 10 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『ハクティビストグループがランサムウェア GhostLocker を発表』

- 2023 年 10 月上旬、新たなランサムウェア「GhostLocker」が発表された。このランサムウェアの開発に関わったのは、テロ組織等様々な勢力と戦うハクティビストとして知られるハッカーグループ GhostSec である。
- 発表に先立つ 8 月末に GhostSec を含む、背景の異なるハッカーグループが結束して「The Five Families」が設立された。ランサムウェア「GhostLocker」のリリースは The Five Families のメンバーによって宣伝されている。
- ハクティビスト GhostSec がどのような形で自らの活動と RaaS を結び付けていくのかは現時点で不明であるが、従来のカテゴリーに留まらない動きは今後のハッカー界の流れの一つを示している可能性が考えられる。

第 2 章『Cisco の IOS XE にゼロデイ脆弱性、4 万台以上に不正プログラムが設置される』

- 10 月 16 日、米ネットワーク大手 Cisco Systems は「Cisco IOS XE」のゼロデイ脆弱性を発表した。攻撃者が本脆弱性を悪用すると、特権アカウントを作成し、機器の制御を奪い、不正プログラムを設置することができる。
- この攻撃により不正プログラムが設置されたとみられる IOS XE 端末が、インターネット上に 4 万台以上発見された。
- 同 OS を含むシステム管理用のインターフェイスはインターネットに公開する必要はない。これを機に、必要最小限のサービスのみがインターネットに公開され、適切なアクセス制御が行われているか、改めて確認することを推奨する。

第 3 章『パレスチナにおける武力衝突とサイバー攻撃』

- 2023 年 10 月のパレスチナにおける武力衝突の開始直後から、パレスチナ/イスラエル各陣営に賛同するハクティビストたちにより、対立組織やその支援国への DDoS や情報暴露等のサイバー攻撃が多数行われている。
- 発電所や小麦粉生産工場といった民間人の生命に関わる重要インフラのシステムへの、機能停止や破壊を狙った攻撃も行われている。
- 野放しなハクティビズムを背景に、紛争下での重要インフラへのサイバー攻撃に歯止めが掛からない。

© NTT Security Holdings

1. ハクティビストグループがランサムウェア GhostLocker を発表

1.1. 概要 [1] [2]

2023 年 10 月上旬、新たなランサムウェア「GhostLocker」が発表された。このランサムウェアの開発に関わったのはハッカーグループ GhostSec で、ISIS 等のテロ組織やロシア等の強権的国家と戦うハクティビストとして知られていた。

GhostLocker の発表に先立ち、GhostSec 他 4 つのハッカーグループは The Five Families を結成しており、ハッカーグループの連携が新たな局面を迎えた可能性がある。

1.2. The Five Families の結成

2023 年 8 月末、GhostSec、SiegedSec、ThreatSec、Blackforums、Stormous の 5 つのハッカーグループが集結して、「The Five Families」を設立したことを発表した。この組織の活動目的については明らかにされていない。

The Five Families に集まった各グループは、ハクティビズムによる政治的要求やランサムウェア攻撃による金銭的利益、あるいは興味本位のいたずらの実行等、活動の方向性や主義主張の濃淡が異なる。

ちなみに、この名称は、かつてニューヨークで大きな勢力を誇ったイタリア系マフィアの Five Families にヒントを得た可能性が考えられる[3]。

【GhostSec について】

GhostSec は、アノニマスの一派として 2015 年から活動が確認できるハッカーグループで、サイバー空間でテロリズムと戦うことを標榜し、Web サイトへの攻撃やインターネット上でのテロリストの募集やプロパガンタの拡散の監視、妨害などを行っていた[4,5]。

2015 年 7 月にはチュニジアやニューヨークでのテロ攻撃の情報を捜査機関に提供し、テロを未然に防止することに成功した[6]。このグループはこれを契機に捜査機関と連携して効率的かつ合法的にテロと戦うことを決定し、Ghost Security Group と改名することにした。しかし、一部のメンバーは元の GhostSec の名前を使って非合法の活動を続けることを選択し、袂を分かった[7]。

---

[1] 出典：Cyberint『GhostLocker: The New Ransomware On The Block』
https://cyberint.com/blog/research/ghostlocker-the-new-ransomware-on-the-block/

[2] 出典：Cyberint『GhostSec Raising the Bar』
https://cyberint.com/blog/research/ghostsec-raising-the-bar/

[3] 出典：SOCRadar『The Five Families: Hacker Collaboration Redefining the Game』
https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

[4] 出典：Cyberint『GhostSec Raising the Bar』
https://cyberint.com/blog/research/ghostsec-raising-the-bar/

[5] 出典：ALTIMETRIK『Behind the Mask of GhostSec: Vigilante Hackers on a Cyber Crusade』
https://www.altimetrik.com/behind-the-mask-of-ghostsec-vigilante-hackers-on-a-cyber-crusade/

[6] 出典：Security Affairs『ANONYMOUS'S TEAM GHOSTSEC THWARTS ISIS TERROR PLOTS』
https://securityaffairs.com/38860/cyber-crime/ghostsec-thwarts-isis-terror-plots.html

[7] 出典：MIC『Anonymous Divided: Inside the Two Warring Hacktivist Cells Fighting ISIS Online』
https://www.mic.com/articles/129679/anonymous-vs-isis-how-ghostsec-and-ghost-security-group-are-targeting-terrorists#.t7BdOvX5w

© NTT Security Holdings

GhostSec はロシアがウクライナに侵攻すると、ウクライナ支持を表明し、攻撃を開始した[8]。2022 年 5 月にロシアの地下鉄システムの制御盤のコントロールを奪い、長期間停止させた後[9]、7 月にはロシアの水力発電所の ICS（産業用制御システム）の制御を掌握し、爆発事故を引き起こしたと主張した[10]。また、同年 10 月、ヒジャブを適切に着用していない女性が警察に拘束され死亡した事件に抗議して、イランの SCADA システムへの攻撃を実施した[11]。2023 年 4 月には、イスラエル警察がイスラム教の聖地アル・アクサー・モスクに突入したことに抗議して、衛星システムと給水ポンプシステムをハッキングしたと主張した[12]。

これらのことから GhostSec は、政治的主張と共に非合法で物理システムに影響を与えるようなハッキングを継続的に行う過激なハクティビストとして、知られている。

【SiegedSec について】[13, 14, 15, 16, 17]

SiegedSec は、2022 年のロシアのウクライナ侵攻の数日前にハクティビスト「YourAnonWolf」が率いる形で出現し、ウクライナ支持を表明している。若いメンバーで構成されたこのグループのチャットチャンネルには、攻撃とは別にカジュアルな会話やジョークもたくさん出ており、ハクティビスト活動から個人的な利益を目的とした悪質なサイバー犯罪まで、様々な攻撃の動機を示している。攻撃手法は、基本的な SQL インジェクションとクロスサイトスクリプティング（XSS）を用いた、Web サイトの改ざんや機密情報への不正アクセスなどである。

攻撃事例としては、2023 年 7 月に NATO が管理するポータルを侵害し、多数の機密情報を盗み出すことに成功している。

イベントに乗じたハッキング活動も見られ、2023 年 2 月のバレンタインには、オーストラリアのソフトウェア会社 Atlassian に「Will you be my valentine?」とテレグラム上で呼びかけてハッキングを宣言し、Atlassian 社のフロア図と従業員情報をリークした。また、同年のハロウィーンでは、イスラエル最大の通信会社 Bezeq に対しサイバー攻撃「Haloween Hack」を行い、同社の約 5 万人の顧客情報をリーク。更に、イスラエル全土を監視するポータルをシャットダウンし、現地のインフラのみならず、リンクされている他国のイスラエル大使館のシステムにも影響を与えた。最後に、Bezeq 社の顧客にいたずらと思われるメー

---

[8] 出典：Cyberint『GhostSec Raising the Bar』
https://cyberint.com/blog/research/ghostsec-raising-the-bar/

[9] 出典：The Tech Outlook『Russian trains still not in function after being hacked by GhostSec』
https://www.thetechoutlook.com/news/technology/russian-trains-still-not-in-function-after-being-hacked-by-ghostsec/

[10] 出典：OTORIO『Targeting ICS with Country-Specific Tactics: Illuminating GhostSec』
https://www.otorio.com/blog/country-specific-ics-targeting-shining-a-light-on-ghostsec/

[11] 出典：Industrial Cyber『OTORIO reveals GhostSec hacktivist group now targets Iranian ICS in support of Hijab protests』
https://industrialcyber.co/news/otorio-reveals-ghostsec-hacktivist-group-now-targets-iranian-ics-in-support-of-hijab-protests/

[12] 出典：ALTIMETRIK『Behind the Mask of GhostSec: Vigilante Hackers on a Cyber Crusade』
https://www.altimetrik.com/behind-the-mask-of-ghostsec-vigilante-hackers-on-a-cyber-crusade/

[13] 出典：SOCRadar『Threat Actor Profile: SiegedSec』
https://socradar.io/threat-actor-profile-siegedsec/

[14] 出典：Cyberint『SiegedSec Compromise NATO』
https://cyberint.com/blog/research/siegedsec-compromise-nato/

[15] 出典：Bleeping Computer『Atlassian data leak caused by stolen employee credentials』
https://www.bleepingcomputer.com/news/security/atlassian-data-leak-caused-by-stolen-employee-credentials/

[16] 出典：The CYBER EXPRESS『SiegedSec Halloween Hack Announcement: Takes Down Bezeq』
https://thecyberexpress.com/bezeq-data-breach-halloween-hack/

[17] 出典：DarkOwl『Dark Web Cyber Group Spotlight: SiegedSec』
https://www.darkowl.com/blog-content/darkowl-cyber-group-spotlight-siegedsec-and-leaked-data/

© NTT Security Holdings

ルを送信し、受信者を困惑させた。

図 1 バレンタインのハッキングの投稿（Telegram より）[18]

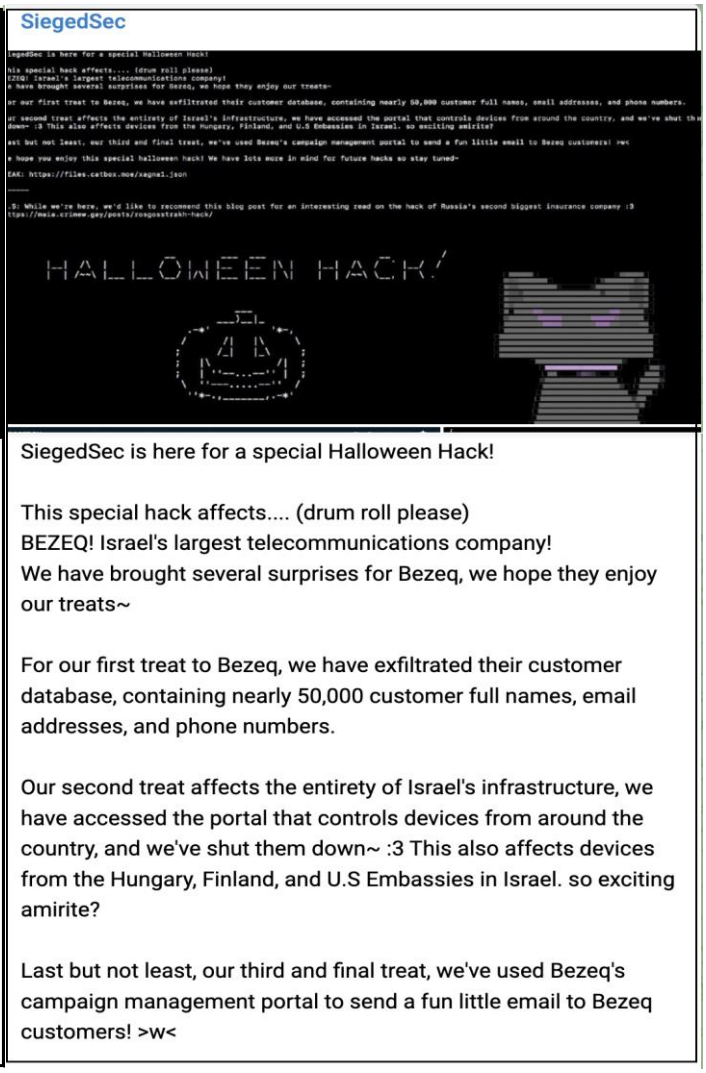

図 2 ハロウィーンのハッキングの投稿（Telegram の一部より）

【ThreatSec について】

2023 年 6 月から活動を確認できる比較的新しいハッカーグループ。イスラエルとパレスチナの紛争について、戦争が嫌いなため両者を攻撃する、とテレグラムで発信。2023 年 10 月にガザ地区に拠点を置く ISP の ALFANET が所有するサーバーを乗っ取って、システムに障害を与えたと主張している[19]。

【Blackforums について】

ハッキングやリークデータの投稿を扱うハッカーフォーラムに集うハッカーグループ。技術的探求心や仲間内での功名心、金銭

[18] 出典：Bleeping Computer『Atlassian data leak caused by stolen employee credentials』
https://www.bleepingcomputer.com/news/security/atlassian-data-leak-caused-by-stolen-employee-credentials/

[19] 出典：SecurityWeek『Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks』
https://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/

© NTT Security Holdings

などがハッキングの動機と考えられる。

【Stormous について】

2021 年にアラビア語話者で結成されたランサムウェアグループであり、暴露サイトを持っている。ロシアのウクライナ侵攻に関して、ロシア支持を表明している。

1.3. ランサムウェア「GhostLocker」

10 月上旬、Telegram のチャンネル GhostLocker で、同名のランサムウェアのリリースが発表され、この後、The Five Families のメンバーによって宣伝が拡散された。投稿内容から、開発の中心となったのは GhostSec と考えられる。また、Stormous は自身のオペレーションで、これまで利用していた StormousX に加えて、GhostLocker も採用することを発表している。

GhostLocker は Ransomware as a Service（RaaS）として、月額サブスクリプションも取り入れた低価格で提供されている。また、このサービスには、マルウェアがセキュリティ対策ソフトウェアでの検出を回避する機能や、下図のように攻撃の状況を管理するためのパネルも含まれている。

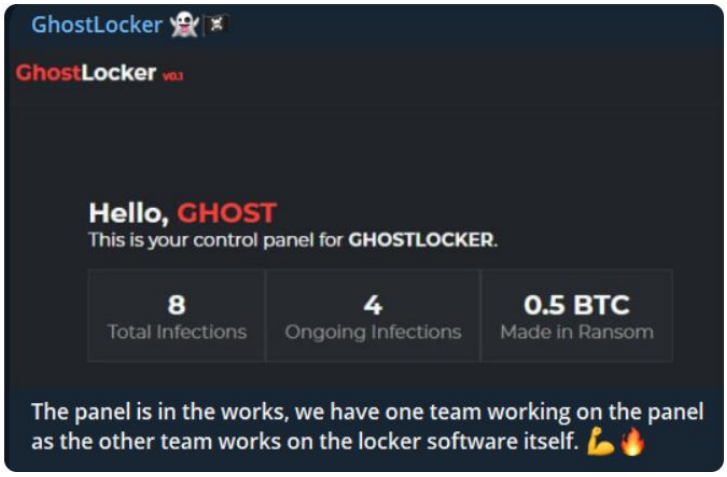

図 3 GhostLocker の管理パネル[20]

GhostLocker のマルウェアが実行されると、ターゲットのデータは強力なアルゴリズムで暗号化され、ファイル名に「.ghost」の拡張子が付加されてアクセスできなくなる。復号するためには被害者は身代金を支払う必要があるが、攻撃者に 48 時間以内に連絡をしないと増額され、支払わないとデータは完全に削除される。また、身代金のメモは、暗号化されたファイル名の変更やサードパーティーの復号ツールの使用、法執行機関や第三者への関与があった場合はデータを完全削除することを示唆している[21]。

[20] 出典：SOCRadar『GhostLocker: A New Generation of Ransomware as a Service (RaaS)』
https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

[21] 出典：PCrisk.com『GhostLocker (.ghost) ransomware virus – removal and decryption options』
https://www.pcrisk.com/removal-guides/28068-ghostlocker-ransomware

© NTT Security Holdings

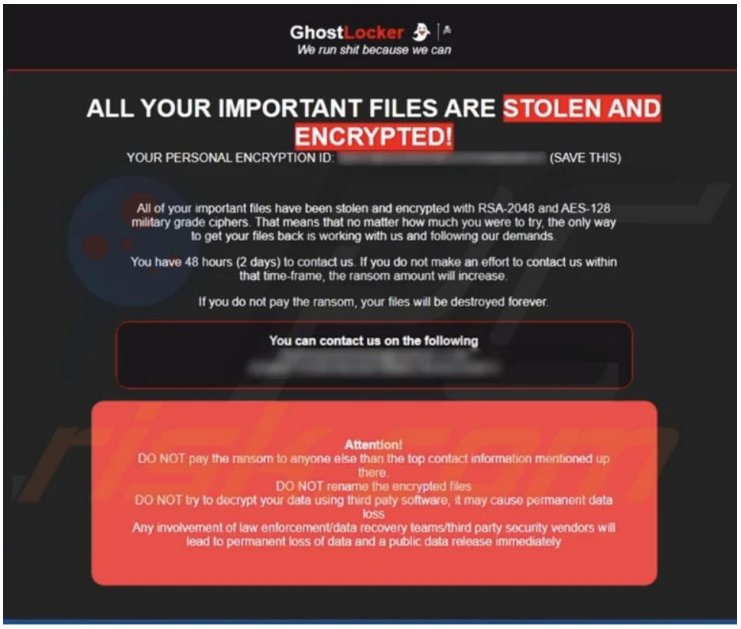

図 4 GhostLocker 実行後に表示される画面（身代金のメモを含んでいる）[22]

1.4. まとめ

ハクティビスト GhostSec が向き合うのは、テロリズムや戦争などであり、これらと戦う中で GhostSec の活動は過激さを増し、ついにはサイバー犯罪グループと連携したり、RaaS を提供したりするまでに至った。この背景として、ウクライナ侵攻や、イスラエルとハマスの軍事衝突などの地政学的あるいは宗教的な対立のエスカレーションにより、ハッカー活動/運動が活性化し、前述のようなハッカーのカテゴリーを越えるような動きが今後も出てくる下地が整いつつある状況があると考える。GhostSec がどのような形で自らの活動と RaaS を結び付けていくのかは未だ見えておらず、単純に金銭を目的としたものなのかどうかは不明である。

また、個人で実行できる DDoS や改ざんなどと違って、ランサムウェアサービスのオペレーションは複雑であり、ContiLeaks（2022 年にロシア支持のランサムウェア集団 Conti の内部状況が、ウクライナ研究者を名乗る人物により暴露された事件）で明らかになったように、組織的に整備された多数の人員を必要とする。このようなサービスをハッカーグループあるいはそのグループ間の連携で運用することは困難が伴うと想像されるため、安定して提供できるかどうかは未知数である。

このグループの活動は先鋭的であり、従来のカテゴリーに留まらない動きは今後のハッカー界の流れの一つを示している可能性が考えられる。

[22] 出典：PCrisk.com『GhostLocker (.ghost) ransomware virus – removal and decryption options』 https://www.pcrisk.com/removal-guides/28068-ghostlocker-ransomware

© NTT Security Holdings

2. Cisco の IOS XE にゼロデイ脆弱性、4 万台以上に不正プログラムが設置される

2.1. 概要

10 月 16 日、米ネットワーク大手 Cisco Systems（以下、「Cisco 社」）は同社のネットワーク機器用 OS である「Cisco IOS XE」の脆弱性を発表した。同 OS の Web 管理インターフェイスがインターネットに公開されている場合、攻撃者は本脆弱性を悪用して、最上位の特権アカウントを作成し、機器の制御を奪うことができる[23]。この発表が行われた時点で、すでに実際の攻撃での悪用が確認されていた。

同日、米国の CISA は「既知の悪用された脆弱性一覧（Known Exploited Vulnerabilities）」に本脆弱性を追加し、注意喚起を行った[24]。これに続き 18 日、日本の JPCERT/CC も注意喚起を発表した[25]。

図 5 JPCERT/CC の注意喚起

2.2. IOS XE と脆弱性について

【IOS XE】

「Cisco IOS XE」は、Cisco 社のオペレーティングシステム「Cisco IOS」シリーズの 1 つで、Linux をベースにしている。同社のルーターやスイッチ等のネットワーク機器で幅広く利用されている[26]。インターネット上に公開されている IOS XE のデバイスは、米国を中心に世界中でおおよそ 15 万台が確認されている[27]。

---

[23] 出典：Cisco Systems『Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature』
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

[24] 出典：CISA『CISA Adds One Known Exploited Vulnerability to Catalog』
https://www.cisa.gov/news-events/alerts/2023/10/16/cisa-adds-one-known-exploited-vulnerability-catalog

[25] 出典：JPCERT/CC『Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起』
https://www.jpcert.or.jp/at/2023/at230025.html

[26] 出典：Cisco Systems『Cisco IOS XE』
https://www.cisco.com/c/ja_jp/products/ios-nx-os-software/ios-xe/index.html

[27] 出典：Bleeping Computer『Over 40,000 Cisco IOS XE devices infected with backdoor using zero-day』
https://www.bleepingcomputer.com/news/security/over-40-000-cisco-ios-xe-devices-infected-with-backdoor-using-zero-day/

© NTT Security Holdings

【CVE-2023-20198 と CVE-2023-20273】[28]

発表された脆弱性は、IOS XE で Web UI（図 6）が有効になっている機器に影響を与える。Web UI は IOS XE に組み込まれており、同 OS 上で HTTP もしくは HTTPS サーバーが有効になっていれば、追加の設定やライセンスを導入する必要なく利用できる。このため、少なくない数のユーザーがこの脆弱性の影響を受けていると考えられる。

Cisco 社の調査によると、実際に被害を受けた IOS XE には攻撃者によって特権アカウントが作成され、不正プログラムが設置されていた。この攻撃には 2 つの脆弱性が利用されていた。攻撃者はまず、脆弱性「CVE-2023-20198」で、リモートから新規のユーザーアカウントを作成。その後、さらに別の脆弱性「CVE-2023-20273」を利用し、そのアカウントを特権ユーザーへと昇格させ、機器の制御を奪い、不正プログラムを設置していた。

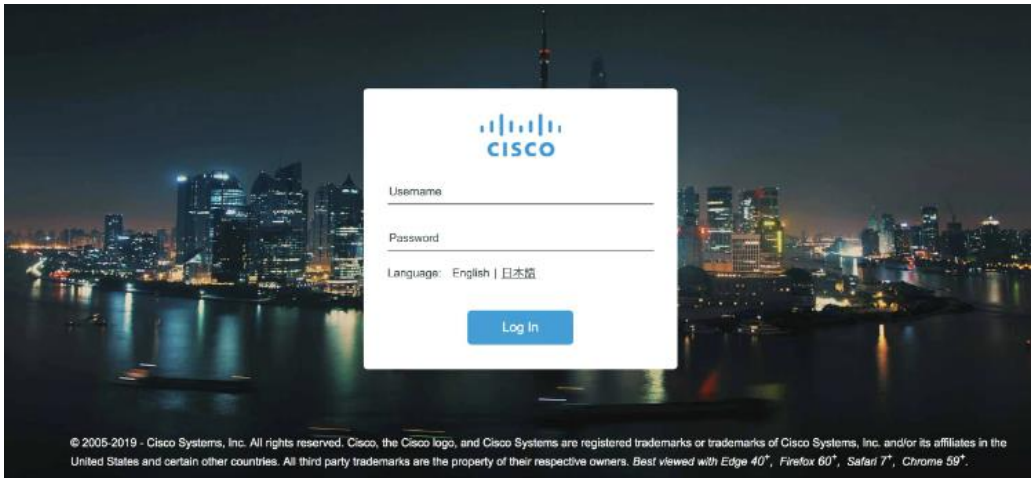

図 6 IOS XE の Web UI ログイン画面

この脆弱性はハッカー達の間でも話題になり、ハッカーフォーラムでも議論されている。

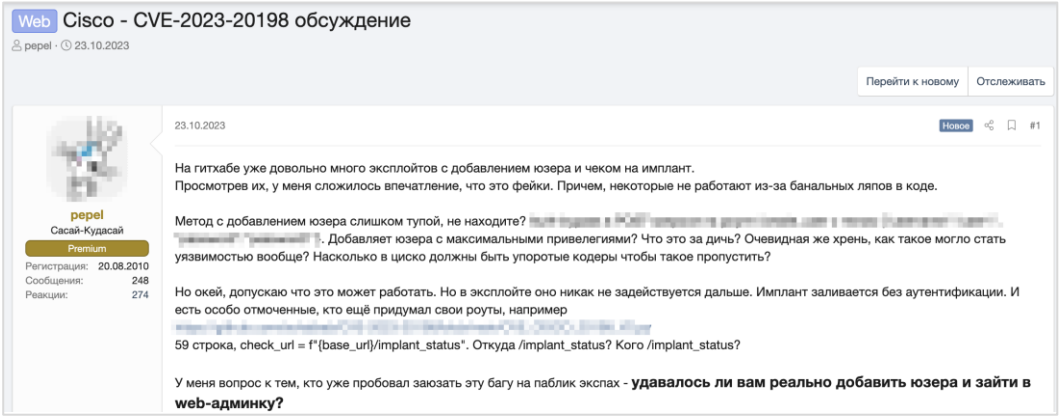

図 7「Cisco - CVE-2023-20198 ディスカッション」と題されたロシア系ハッカーフォーラムのスレッド

なお、本脆弱性の発表から 6 日後の 10 月 22 日、Cisco 社はこれらの脆弱性を修正するバージョンの提供を開始した。

[28] 出典：Cisco Systems『Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature』
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

© NTT Security Holdings

【攻撃と被害状況】

攻撃によって不正プログラムが設置されている IOS XE に特定のリクエスト（図 8）を送信すると、16 進数で 18 文字の文字列が返される。この挙動を利用したセキュリティ会社の調査によると、不正プログラムが設置された IOS XE が 10 月 18 日には 41,983 台発見されている[29]。

```
curl -k -X POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"

If the request returns a hexadecimal string, the implant is present.
```

図 8 不正プログラムを確認するリクエストを送信するコマンド（Cisco 社の発表より）
「16 進数の文字列が返された場合、不正プログラムが存在する」

```
% curl -k -X POST "http://[redacted]/webui/logoutconfirm.html?logon_hash=1"
[redacted]ffeeabbd5c[redacted]
```

図 9 不正プログラムが設置された機器にリクエストを送信した例（赤枠内が機器から返されたレスポンス）

なお、機器が再起動されると、埋め込まれた不正プログラムは削除されるが、作成された特権アカウントは有効なまま残る。16 進数の文字列が返ってこなかったとしても、攻撃を受けていないことにはならないため、注意が必要である。

2.3. 管理インターフェイスを公開するリスク

IOS XE に限らず、管理インターフェイスはインターネットに公開すべきではない。特に、攻撃者はネットワーク内への侵入の為に、VPN やファイアウォール等の、ネットワークへの入り口にあたる重要なシステムの管理インターフェイスを狙ってくる。

管理インターフェイスに対する攻撃手法として、ブルートフォース攻撃などによる認証試行のほか、脆弱性を攻撃するコードの送信が挙げられる。これらの攻撃が成功すると、管理者の権限でユーザーの追加や設定の変更等が行われる。最終的に組織のネットワーク内に侵入され、情報窃取やランサム被害等へと繋がる恐れがある。

6 月、米国の CISA はこのような攻撃により被害が続出したことを踏まえ、米政府機関に対して「BOD 23-02（Binding Operational Directive, 拘束力のある運用指令）」を発し、管理インターフェイスに対して外部からアクセスできないようにする等の対策を行うことを義務付けた[30]。

2.4. まとめ

今回のゼロデイ攻撃により、4 万台以上のデバイスが被害を受けた。システム管理用のインターフェイスはインターネットに公開すべきでないことが、本件から改めて明らかになった。これを機に、必要最小限のサービスのみがインターネットに公開され、適切なアクセス制御が行われているか、改めて確認することを推奨する。

---

[29] 出典：Censys『CVE-2023-20198 – Cisco IOS-XE ZeroDay』
https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/

[30] 出典：CISA『BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces』
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02

© NTT Security Holdings

3. パレスチナにおける武力衝突とサイバー攻撃

3.1. 概要

2023 年 10 月 7 日に勃発して以来、パレスチナの武装勢力ハマスとイスラエルの武力衝突が続いている。戦闘開始直後から、両勢力に協力するハクティビストたちによるサイバー攻撃が一気に拡大した [31]。DDoS 攻撃が多数行われる他、情報漏洩による暴露やサイト改ざん、さらには重要インフラを狙った攻撃にまでエスカレートしている。

民間に関わる重要インフラへのサイバー攻撃は国際人道法に違反するおそれがある。だが、違反による処罰の実効性は薄く、主義主張を優先するハクティビストたちは歯止めなく攻撃を展開している。

3.2. 勃発直後から発生したサイバー戦

武力衝突の直後から、サイバー攻撃が発生している[32, 33]。戦闘の口火はハマスのロケット弾の大量発射により切られた。イスラエルにはロケット弾攻撃の警戒情報を民間に提供するサイトがあるが、攻撃開始約 12 分後には、そのサイトに対する DDoS 攻撃が検知された[34]。その後、新聞等の報道メディア、コンピューターソフトウェア業界、政府機関のサイトへ DDoS 攻撃が広がっていった。なお、イスラエル側だけでなくパレスチナ側の Web サイトに対する DDoS 攻撃も検知されており、あるサイトでは一時、全トラフィックのうち 60%を攻撃関連のトラフィックが占めた[35]。

このようなサイバー攻撃の主な実行者が、ハクティビストである。DDoS 攻撃後に犯行声明を出す威力妨害が盛んな他、サイトを改ざんしてメッセージを掲載する攻撃や、機密情報を窃取して暴露するといった攻撃も行われている。またパレスチナ/イスラエルの当事者だけでなく、国外のハクティビストが両勢力それぞれに助太刀する攻撃が、数多く確認されている。長年くすぶり続けるパレスチナ問題を背景にしたハクティビストの活動は以前から存在していたが、今回の武力衝突をきっかけに一気に活発化した。

【親パレスチナのハクティビスト】

親パレスチナのハクティビストのグループは 130 グループ以上[36]あり、その多くは中東やアジア（インドネシア、マレーシア等）のイスラム圏のグループであると称している。

これらのグループは、パレスチナのイスラム教徒への連帯から、反イスラエルを掲げている。さらに、イスラエル本国だけではなく親イスラエルの立場をとる欧米等の国々にも攻撃対象を広げている。特に、パキスタンやバングラデシュといったアジアのイスラム教

---

[31] 出典：Reuters『Hacktivists stoke Israel-Gaza conflict online』
https://www.reuters.com/world/middle-east/hacktivists-stoke-israel-gaza-conflict-online-2023-10-11/

[32] 出典：FalconFeeds『The Evolving Landscape of Cyber Warfare in the Israel-Palestine Conflict: A Comprehensive Analysis』
https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011

[33] 出典：SOCRadar『Reflections of the Israel-Palestine Conflict on the Cyber World』
https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/

[34] 出典：Cloudflare『Internet traffic patterns in Israel and Palestine following the October 2023 attacks』
https://blog.cloudflare.com/internet-traffic-patterns-in-israel-and-palestine-following-the-october-2023-attacks/

[35] 出典：Cloudflare『Cyber attacks in the Israel-Hamas war』
https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

[36] 出典：X『@Cyberknow20』
https://x.com/Cyberknow20/status/1720217982201409821

© NTT Security Holdings

圏のグループによる、緊張関係にあるインドへの攻撃活動が目立つ。

【日本にも及ぶハクティビストの攻撃】

様々なグループが日本を攻撃対象としている。10 月 16 日に国連の安全保障理事会でロシアが提出した停戦案に日本が反対して以来、イスラエルを支援する国々の一つに日本が挙げられるようにになった。

まず 10 月 20 日に、日本の政府機関等のウェブサイトが複数、親パレスチナのグループによる DDoS 攻撃のターゲットリストに掲載された。10 月 25 日には日本の事業者のサイトが、バングラデシュ系のグループによってパレスチナを支持するメッセージの画面へと改ざんされた[37]。11 月 1 日には日本の政府機関等に DDoS 攻撃を実施したと、パキスタン系のグループが発表した。

【親イスラエルのハクティビスト】

親イスラエルのハクティビストも、20 グループ以上[38]と、親パレスチナには及ばないが複数確認されており、特にインドのグループによる活動が目立つ。パレスチナ側への DDoS 攻撃の他、ハマスのサイトの改ざんをしたといった主張や、パレスチナの医療施設から窃取したという医療データの暴露といった攻撃も確認されている。

3.3. 重要インフラを狙うハクティビストの活動

ハクティビストの中には、重要インフラに関わる制御システムを狙った攻撃を企むグループも確認されている。

例えば、イスラエルの水道施設を制御するシステムへの侵入に成功したと、親パレスチナの複数のグループが発表している（図 10、図 11）。別のグループは、10 月半ばにイスラエルの発電所へサイバー攻撃を実行し、給電を止めることに成功したとの発表を（図 12）、さらに 11 月初めにはイスラエル最大の小麦粉生産工場のシステムに侵入したとの発表をした（図 13）。このグループは重要インフラへの攻撃の他にも、イスラエルの組織に対しランサムウェア攻撃を実行したとの声明も出している [39]。

もし重要インフラに関わるシステムが、ランサムウェア攻撃・復元のできないワイパー攻撃等により破壊された場合、電気・生活用水・食料等の長期的な供給停止が発生し、民間人の生命を脅かしかねない。

[37] 出典：NHK『東京のペットサロンでも…中東の軍事衝突でサイバー攻撃相次ぐ』
https://www3.nhk.or.jp/news/html/20231026/k10014237901000.html

[38] 出典：FalconFeeds『The Evolving Landscape of Cyber Warfare in the Israel-Palestine Conflict: A Comprehensive Analysis』
https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011

[39] 出典：Security Affairs『Pro-Palestinian hackers group 'Soldiers of Solomon' disrupted the production cycle of the biggest flour production plant in Israel』
https://securityaffairs.com/153778/security/soldiers-of-solomon-hacked-israel-flour-plant.html

© NTT Security Holdings

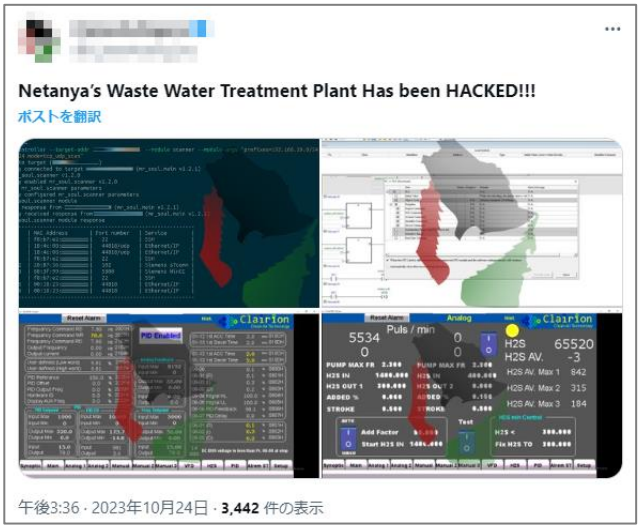

図 10 水道施設への攻撃を示唆する投稿

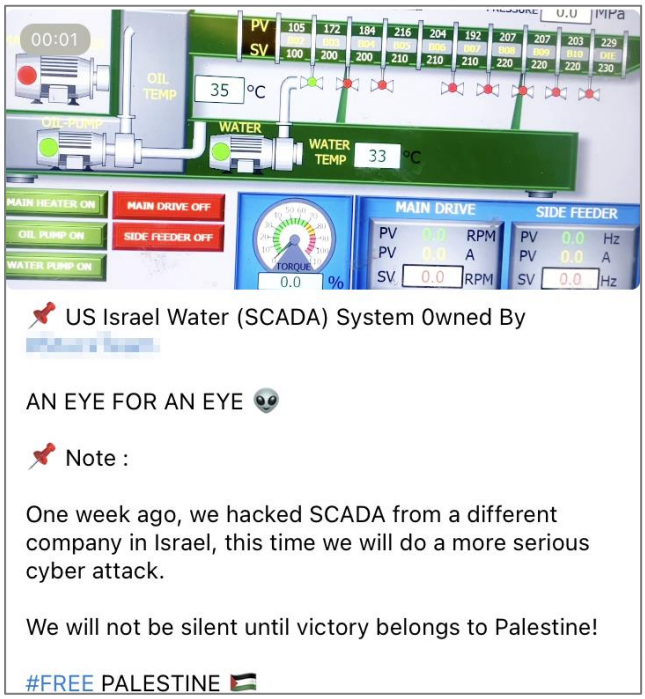

図 11 水道施設への攻撃を主張する投稿

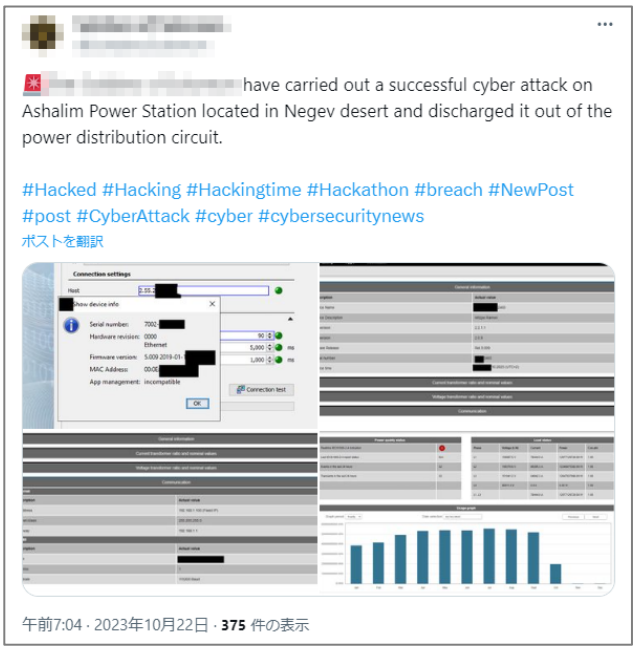

図 12 発電所への攻撃を示唆する投稿

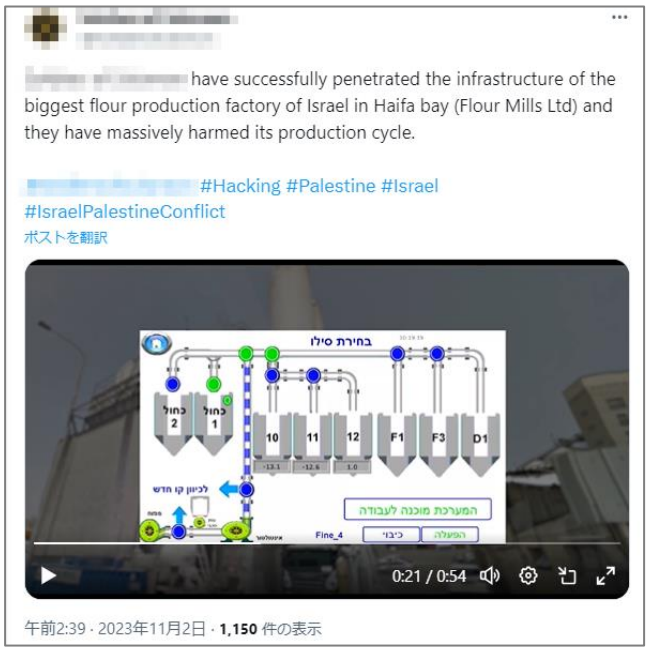

図 13 小麦粉生産工場への攻撃を示唆する投稿

3.4. 赤十字国際委員会（ICRC）が提案するサイバー攻撃のルール

パレスチナでの軍事衝突勃発の直前、10 月 5 日に赤十字国際委員会（ICRC）が、戦争中の民間ハッカーの行動についてのルールを提案していた[40]。ロシアによるウクライナ侵攻後から盛んになった民間のハッカーによる放埒な活動への危機感を

[40] 出典：ICRC Humanitarian Law & Policy Blog『8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them』 https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/

© NTT Security Holdings

背景としている。

このルールは、国際人道法に違反する、軍事標的以外の民間を標的とする行為の抑制を目的としている。民間の重要インフラや病院等へのサイバー攻撃の禁止、そして、たとえ敵がこのルールに従わない場合でも遵守することを求めている。また ICRC は国家に対しても、国際人道法における交戦規則の順守という観点から、ルールを逸脱しないよう自国の民間ハッカーの活動を制限することを要請している。国際人道法においては、重要インフラに被害を与えるようなサイバー攻撃をハクティビストが行った場合、捕虜として身分を保障される軍人とは異なり、民間人であるため犯罪者またはテロリストとして国際的に訴追を受ける可能性がある。

だが、発表直後よりウクライナ・ロシア双方のハクティビスト達からは、ルールに否定的な反応が見られた。メディアからのインタビューに対し、ルールを破るのはグループの大義のために不可避という回答が有ったほか[41]、ロシアの赤十字協会のサイトを改ざんすることで反対の声明を発表した、親ウクライナのハクティビストもいた[42]。

3.5. まとめ

武力衝突をきっかけに各勢力を支持するハクティビストの活動が一気に活発化した。真偽不明なものもあるが、重要インフラへの攻撃も躊躇なく行われている。被害施設の機能喪失により人命に影響が及ぶと、重大な犯罪やテロ行為に該当する可能性がある。親パレスチナのハクティビストは、イスラエル以外にも米国の民間・公共インフラへの攻撃を世界中のハッカーに呼びかけており[43]、このような重要インフラを狙った攻撃が武力衝突に直接関連していない国にも行われていく恐れがある。

ハクティビストは、先進国においては 2010 年代後半から法執行機関よるサイバー犯罪の取り締まりが進んだことで、減少していると言われている。一方で、多くの発展途上国では依然としてハクティビストの活動が野放しであり、これが、パレスチナ側からのサイバー攻撃が活況を呈する一因となっている。サイバー空間の非対称戦は、イスラエルが物資や戦力で圧倒する物理空間と真逆の方向性を示しているようである。

以上

[41] 出典：BBC News『Rules of engagement issued to hacktivists after chaos』
https://www.bbc.com/news/technology-66998064

[42] 出典：The Record『'War has no rules': Hacktivists scorn Red Cross' new guidelines』
https://therecord.media/hacktivists-respond-to-red-cross-rules-with-ridicule

[43] 出典：X『@FalconFeedsio』
https://twitter.com/FalconFeedsio/status/1711033041827828087

© NTT Security Holdings

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス： WA_Advisorysupport@ntt.com

© NTT Security Holdings