MANDIANT

The Defender's Advantage Cyber Snapshot (Istantanea informatica sul vantaggio del difensore)

The Defender's Advantage Cyber Snapshot (Istantanea informatica sul vantaggio del difensore) offre approfondimenti su argomenti di difesa informatica di crescente importanza basati su osservazioni in prima linea Mandiant ed esperienze reali. Gli argomenti trattati in questo numero includono il modo in cui gli aggressori vedono le organizzazioni, le minacce alla tecnologia operativa, le fusioni e le acquisizioni e la protezione da eventi di ampio impatto.

› **Rilevamento dei percorsi di exploit più comunemente esposti su Internet** 3

› **Raccolta di dati per scoprire le minacce della tecnologia operativa** 8

› **Due diligence tecnica per fusioni e acquisizioni** 14

› **Protezione degli eventi sociali mentre tutto il mondo sta guardando** 16

Rilevamento dei percorsi di exploit più comunemente esposti su Internet

Fonte di dati

I dati sui problemi a cui si fa riferimento provengono direttamente da Mandiant Advantage Attack Surface Management e riguardano 21.092 raccolte di clienti. Il set di dati comprende 21.392 problemi identificati dal 1º gennaio 2022 al 31 marzo 2022, con gravità elevata o critica. I problemi sono un sottoinsieme di raccolte dei clienti, che contengono l'inventario delle risorse e le tecnologie associate in esecuzione su superfici di attacco esterne. La gravità dei problemi viene assegnata in base al potenziale impatto sul sistema interessato. Nei casi in cui viene identificata una vulnerabilità e un'esposizione comune (CVE), la gravità è legata alla valutazione del rischio da parte di Mandiant Advantage Threat Intelligence.

Un problema è la scoperta di un'attività su una risorsa esterna che richiede ulteriori indagini.

Dal 1° gennaio al 31 marzo 2022, Mandiant ha identificato problemi comuni di gravità elevata e critica che si sono verificati in aziende di medie e grandi dimensioni a causa della mancata applicazione di patch alle tecnologie e di una deriva della configurazione delle risorse connesse a Internet. Per questi problemi, Mandiant consiglia vivamente ai team di sicurezza di stabilire un processo per identificare i casi che si verificano all'interno della propria organizzazione e di seguire le strategie di rimedio consigliate.

Categorie di problemi con gravità da elevata a critica

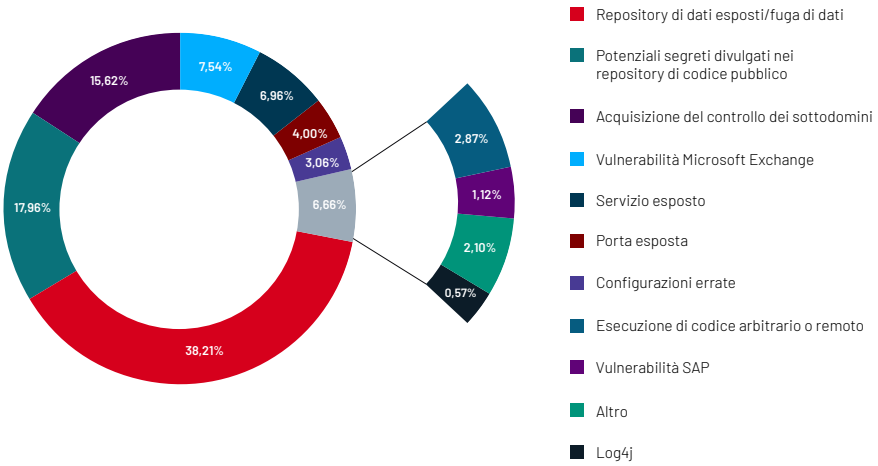

Figura 1. Tutte le categorie di problemi di gravità da elevata a critica osservate da Mandiant Advantage Attack Surface Management (dal 1° gennaio 2022 al 31 marzo 2022).

I problemi includono vulnerabilità, configurazioni errate, indicatori di compromissione (IOC) o fughe di dati di qualsiasi tipo. Mandiant Advantage Attack Surface Management è stato utilizzato per effettuare una ricognizione come farebbe un aggressore, ossia analizzando le risorse e le tecnologie rivolte a Internet e scansionando le fonti di Open Source Intelligence (OSINT) alla ricerca di aree di debolezza, per scoprire i potenziali percorsi che un aggressore potrebbe seguire per sfruttare una risorsa esposta.

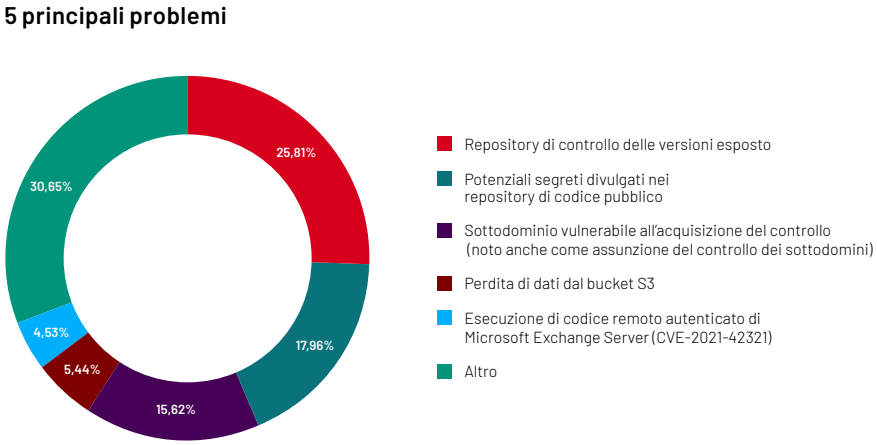

Figura 2. I cinque principali problemi osservati da Mandiant Advantage Attack Surface Management (dal 1° gennaio 2022 al 31 marzo 2022).

Repository di dati esposti e fughe di dati

Qualsiasi organizzazione potrebbe essere colpita da un evento come un repository di dati esposto a causa di configurazioni errate o di una scarsa implementazione dei criteri. Un aggressore sfrutta questa forma di esposizione cercando informazioni all'interno del repository.

Un quarto (25,81%) dei problemi osservati riguardava i repository di controllo di versione esposti. Tipicamente scoperti su server Web pubblici, i repository di controllo delle versioni possono contenere file sensibili e codice sorgente relativi a una determinata organizzazione e/o applicazione. Con questi repository esposti gli aggressori hanno l'opportunità di cercare file di configurazione, dati sensibili o informazioni riservate, tutti elementi che possono essere utilizzati per avanzare nel tentativo di compromettere un'azienda.

Le organizzazioni possono affrontare l'esposizione implementando un processo per garantire che le applicazioni portate in produzione blocchino l'accesso al repository. Quando viene rilevata un'esposizione, è consigliabile avviare un'indagine sul repository, bloccandolo localmente e verificando la presenza di dati e contenuti sensibili.

I bucket S3 esposti (il 5,44% del campione) sono un altro problema comune che affligge le organizzazioni. Mandiant ha osservato due tendenze comuni per le esposizioni dei bucket S3: una configurazione errata che consente l'accesso pubblico e un criterio di bucket che consente inavvertitamente l'accesso non autorizzato a un utente autenticato. In alcuni casi, gli utenti autenticati possono scrivere sul bucket.

Anche con i sofisticati strumenti di configurazione dei provider di servizi cloud, le perdite dei bucket sono ancora un problema comune. Se viene scoperta l'esposizione di un bucket S3, i team di sicurezza devono verificare il livello di esposizione e modificare i criteri per limitare l'accesso.

Potenziali segreti divulgati nei repository di codice pubblico

Le organizzazioni utilizzano sempre più spesso il controllo di versione open-source come Github. Mandiant esegue una scansione continua dei repository pubblici Github, identificando modelli noti di informazioni riservate e sensibili. I potenziali segreti divulgati nei repository di codice pubblico (il 17,96% del campione) indicano una potenziale perdita di credenziali o una modifica del codice sorgente che richiede attenzione immediata. Gli aggressori spesso utilizzano credenziali compromesse per pubblicare codice dannoso che potrebbe avere un impatto devastante sulle comunità open source.

Le organizzazioni a cui è stato segnalato questo tipo di problema devono eseguire una revisione approfondita del codice e avviare una risposta all'incidente.

Acquisizione del controllo dei sottodomini

Configurare i sottodomini affinché puntino a un servizio di terze parti è una pratica comune in quasi tutte le organizzazioni. Tuttavia, i sottodomini abbandonati rappresentano un vettore di rischio sottile, ma importante. I sottodomini abbandonati, che puntano a un provider che consente la configurazione, e il codice possono essere utilizzati per compromettere le credenziali delle sessioni o nelle campagne di phishing. Una pulizia del DNS ottimale può ridurre il rischio che un aggressore utilizzi un sottodominio abbandonato su un servizio di terze parti per scopi dannosi.

Le osservazioni di Mandiant indicano che i sottodomini scoperti (il 15,62% del campione) erano vulnerabili all'acquisizione del dominio. Nella maggior parte dei casi, il sottodominio puntava a un host di terze parti dove non era stato rimosso e forniva meccanismi di registrazione utilizzabili da chiunque. Un aggressore potrebbe quindi rivendicare il sottodominio e ospitare contenuto non attendibile.

Le organizzazioni che ricevono una notifica di problema ad alta gravità in un sottodominio vulnerabile devono adottare le misure appropriate per rivendicare il sottodominio attraverso l'host di terze parti.

Microsoft Exchange

Da marzo 2021, Mandiant ha osservato attacchi mirati e casi di abuso di Microsoft Exchange Server.[1] A partire da marzo 2022, Mandiant continua a osservare una tendenza che indica che i server Exchange rimangono senza patch e vulnerabili a CVE-2021-26855, CVE-2021-31206, CVE-2021-34473, CVE-2021-42321 e una piccola percentuale (<0,01%) è vulnerabile a una web shell affiliata a Hafnium.

Problemi di Microsoft Exchange

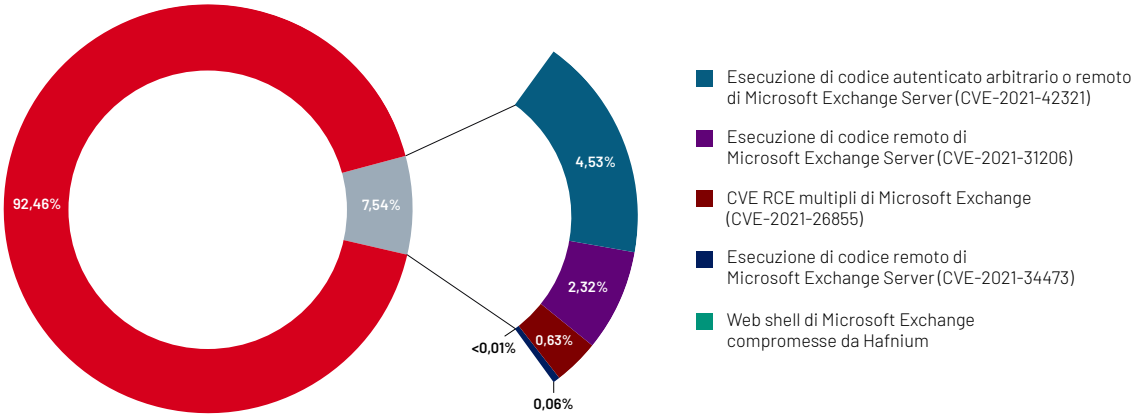

Figura 3. Le vulnerabilità di Microsoft Exchange più diffuse identificate da Mandiant Advantage Attack Surface Management (dal 1° gennaio 2022 al 31 marzo 2022).

1. Mandiant (4 marzo 2021). Rilevamento e risposta allo sfruttamento delle vulnerabilità del giorno zero di Microsoft Exchange.

La Cybersecurity and Infrastructure Security Agency (CISA) ha aggiunto diverse vulnerabilità di Microsoft Exchange al suo catalogo di vulnerabilità sfruttate note e ha stabilito le date necessarie per porvi rimedio.[2] Mandiant consiglia vivamente di scaricare l'aggiornamento di sicurezza appropriato da Microsoft per applicare le patch alle vulnerabilità e rispettare le indicazioni della CISA. Ad esempio:

- CVE-2021-26855[3] aveva una richiesta di correzione per la data 16 aprile 2021
- CVE-2021-31206[4] aveva una richiesta di correzione per la data 17 novembre 2021
- CVE-2021-34473[5] aveva una richiesta di correzione per la data 17 novembre 2021
- CVE-2021-42321[6] aveva una richiesta di correzione per la data 1º dicembre 2021

Tra le vulnerabilità di Microsoft Exchange, la CVE-2021-42321 è la più diffusa nel set di dati Mandiant e rappresenta il 4,53% di tutti i problemi identificati. Mandiant considera questa vulnerabilità ad alto rischio a causa della possibilità che un attore malintenzionato invii un argomento cmdlet dannoso a un server con un ruolo autenticato.

Il 17 marzo 2022, il Federal Bureau of Investigation (FBI) ha rilasciato una comunicazione in cui informa che CVE-2021-26855 e CVE-2021-34473, tra le altre, sono state utilizzate per distribuire il ransomware AvosLocker.[7]

Aggiungere visibilità esterna ai programmi di difesa informatica

Comprendere la superficie di attacco dal punto di vista di un avversario aiuta le organizzazioni a capire quali controlli devono essere testati e quali sono le risorse preziose da valutare. In base alle osservazioni di Mandiant, le risorse tipicamente trascurate all'interno della superficie di attacco sono:

- Servizi di database e di accesso remoto rivolti all'esterno
- Account di sviluppatore su siti come Github o Gitlab
- Ambienti di gestione temporanea e controllo qualità
- Bucket o archiviazione BLOB rivolti all'esterno in un ambiente cloud
- Account di servizio utilizzati per i sistemi rivolti all'esterno
- Software applicativo più esoterico o servizi di rete esposti a Internet
- Sistemi di posta elettronica secondari che possono essere utilizzati per recapitare payload senza filtrare i contenuti

Stabilire una visione completa della superficie di attacco consente di creare profili di minacce informatiche, dare priorità agli aggiornamenti e alle modifiche della configurazione, creare un contesto per i test di penetrazione, rispondere agli incidenti e porvi rimedio.

2. CISA (17 novembre 2021). Il CISA aggiunge al catalogo quattro vulnerabilità sfruttate note.
3. Microsoft Security Response Center (16 marzo 2021). Vulnerabilità dell'esecuzione di codice remoto di Microsoft Exchange Server: CVE-2021-26855.
4. Microsoft Security Response Center (13 luglio 2021). Vulnerabilità dell'esecuzione di codice remoto di Microsoft Exchange Server: CVE-2021-31206.
5. Microsoft Security Response Center (13 luglio 2021). Vulnerabilità dell'esecuzione di codice remoto di Microsoft Exchange Server: CVE-2021-34473.
6. Microsoft Security Response Center (6 dicembre 2021). Vulnerabilità dell'esecuzione di codice remoto di Microsoft Exchange Server: CVE-2021-42321.
7. FBI IC3 (17 marzo 2022). Joint Cybersecurity Advisory: indicatori di compromissione associati al ransomware AvosLocker.

Raccolta di dati per scoprire le minacce della tecnologia operativa

TRITON è un framework di comunicazione ed exploit compilato in Python progettato per colpire i sistemi OT. TRITON è stato impiegato nel 2017 contro i sistemi di sicurezza strumentati di un impianto di infrastrutture critiche con sede in Medio Oriente. Mandiant ha valutato, con elevata affidabilità, che l'attività è stata supportata dall'Istituto Centrale di Ricerca Scientifica di Chimica e Meccanica (CNIIHM noto anche come TsNIIKhM e TsNII), un istituto di ricerca tecnica di proprietà del governo russo con sede a Mosca.

INCONTROLLER è una raccolta di tre strumenti OT separati progettati per attaccare alcuni dispositivi di sistemi di controllo industriale (ICS). Ogni strumento ha funzionalità personalizzate che interagiscono con i server OPC-UA, alcuni controllori logici programmabili (PLC) di Schneider Electric e alcuni dispositivi Omron.

Negli ultimi anni, Mandiant ha osservato un aumento significativo dell'attività delle minacce che possono avere un impatto sulla produzione delle organizzazioni industriali e delle infrastrutture critiche. Queste attività si sono evolute fino a incorporare aggressori opportunisti che prendono di mira la tecnologia operativa (OT) controllata da Internet, bande di ransomware di alto profilo che traggono profitto dall'ostruzione dei sistemi di produzione e gruppi sponsorizzati da Stati nazionali che sviluppano strumenti complessi con il potenziale di mettere in pericolo la sicurezza fisica delle popolazioni umane. Con l'avanzare di queste minacce, la nostra raccolta di informazioni sulle minacce si è adattata.

I metodi di raccolta delle informazioni sulle minacce informatiche sui sistemi OT tradizionali spesso si basano solo su competenze specifiche e sull'analisi qualitativa di alcuni casi di grande impatto come[8] INDUSTROYER.V2[9] o, più recentemente, INCONTROLLER.[10] La creazione di grandi serie di dati sulle minacce OT è stata storicamente difficile. I fattori che hanno contribuito a tale situazione sono la mancanza di visibilità sulle reti di produzione, la mancanza di incentivi per le organizzazioni a condividere le informazioni e la mancanza di consapevolezza dei diversi tipi di attività che possono avere un impatto sui sistemi di produzione. Poiché Mandiant continua a osservare aggressori che prendono di mira l'OT in modi diversi, dagli operatori di ransomware[11] ai crimini di opportunità poco sofisticati[12], la capacità di acquisire dati preziosi aumenta.

Nel corso degli anni, Mandiant ha scoperto importanti dati relativi alle minacce OT nascosti nei repository di malware, nei forum online, nelle pubblicazioni di ricerca e dei media, nelle fughe di notizie sulle estorsioni e in altri luoghi.

La pianificazione e l'attuazione di attacchi per modificare o interrompere la funzionalità prevista dei sistemi OT richiede ampie capacità di raccogliere informazioni sull'obiettivo, ottenere l'accesso alle reti IT e OT, muoversi attraverso i sistemi intermediari e sfruttare le debolezze dei sistemi di produzione. Migliorando la visibilità su diverse fonti di dati, le aziende possono identificare le attività degli aggressori nelle prime fasi del ciclo di vita degli attacchi e impedire che raggiungano i sistemi di produzione.

8. Mandiant (10 aprile 2019). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping.
9. Mandiant (25 aprile 2022). INDUSTROYER.V2: Old Malware Learns New Tricks.
10. Mandiant (13 aprile 2022). INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems.
11. Mandiant (15 luglio 2020). Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families.
12. Mandiant (25 maggio 2021). Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises.

Raccolta e filtraggio dei dati OT

Mandiant rintraccia i dati pertinenti per i difensori dell'OT grazie a un team di ricercatori che lavora su raccolte di intelligence globali, a una solida rete di partner per la condivisione delle informazioni, a incarichi di consulenza e risposta agli incidenti, alla ricerca di minacce da una varietà di fonti e ad altri metodi.

Visualizzazione del panorama delle minacce OT

L'arricchimento dell'intelligence basata sui dati OT e fondata su diverse fonti e metodi di filtraggio, offre a Mandiant visibilità su diverse sfaccettature del panorama delle minacce OT.

Gli aggressori motivati finanziariamente hanno un impatto sulle organizzazioni industriali e le infrastrutture critiche

Negli ultimi due anni, Mandiant ha seguito l'evoluzione degli aggressori di ransomware che hanno avuto un impatto sulla produzione industriale[13] e che hanno ampliato l'accesso ai sistemi OT.[14]Dal 1º aprile 2021 al 31 marzo 2022, Mandiant ha osservato molti casi in cui gli aggressori hanno utilizzato il ransomware per colpire organizzazioni industriali e di infrastrutture critiche in settori che spesso si affidano ai sistemi OT per supportare la produzione.

Per analizzare sistematicamente questa attività, Mandiant ha raccolto informazioni dalle fughe di estorsioni di ransomware, monitorando quasi 1.400 vittime in settori ad alta intensità OT come quello idrico, energetico e manifatturiero. I dati sono stati filtrati per scoprire le seguenti tendenze:

- Il 56% delle vittime proveniva dall'industria manifatturiera e dall'edilizia/ingegneria
- Il 28% delle organizzazioni aveva più di 500 dipendenti
- Le infezioni LockBit e Conti sono state le più prolifiche, responsabili di oltre il 40% delle attività
- Una fuga di notizie di estorsione ransomware su sette di questo sottoinsieme probabilmente conteneva la documentazione OT sensibile[15]

13. Mandiant (24 febbraio 2020). Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT.
14. Mandiant (15 luglio 2020). Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families.
15. Mandiant (31° gennaio 2022) 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information.

Percentuale di vittime per settore primario

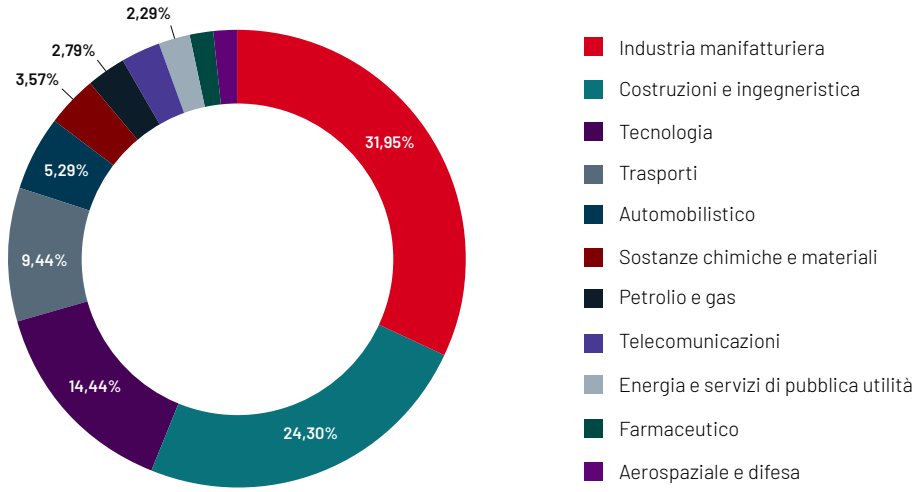

Figura 4. Vittime di ransomware esposte in fughe di estorsione del settore industriale e delle infrastrutture critiche (1º aprile 2021 - 31 marzo 2022).

Dimensioni stimate dell'azienda delle vittime di ransomware

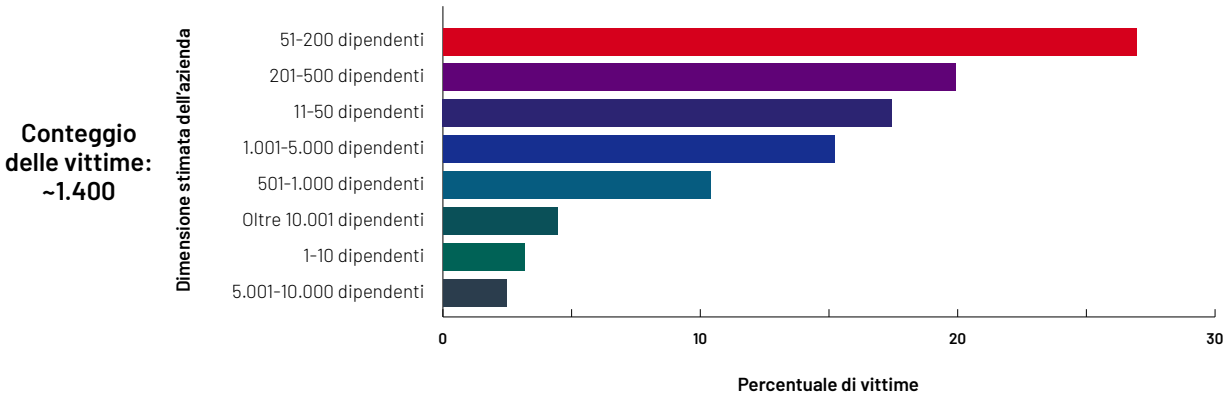

Figura 5. Dimensione stimata delle aziende vittime di ransomware per i settori industriali e delle infrastrutture critiche (1° aprile 2021 - 31 marzo 2022).

L'ampia distribuzione di malware può supportare l'accesso iniziale per le future compromissione dell'OT

Una sfida comune nella sicurezza OT è quella di anticipare le attività delle minacce il più presto possibile nel ciclo di vita dell'attacco. Mandiant concentra quindi gli sforzi sul filtraggio delle attività delle minacce per identificare possibili indicazioni di interesse per compromettere le organizzazioni OT. Tra il 1° aprile 2021 e il 31 marzo 2022, Mandiant ha raccolto e analizzato i contenuti di e-mail di phishing e siti dannosi ampiamente diffusi che contenevano parole chiave relative a settori che utilizzano comunemente sistemi OT. La raccolta di questi dati consente di ottenere una migliore visibilità sugli eventi che possono evolvere in attacchi di maggiore impatto.

Nell'ultimo anno, Mandiant ha rilevato oltre 1.600 e-mail di phishing con contenuti che includevano parole chiave legate al settore OT, come ordine, richiesta, rfq, preventivo, acquisto o fattura. Queste email contenevano anche oltre 2.200 payload che distribuivano oltre 30 tipi di malware ampiamente conosciuti, tra cui AGENTTESLA, EMOTET, FORMBOOK e GULOADER.

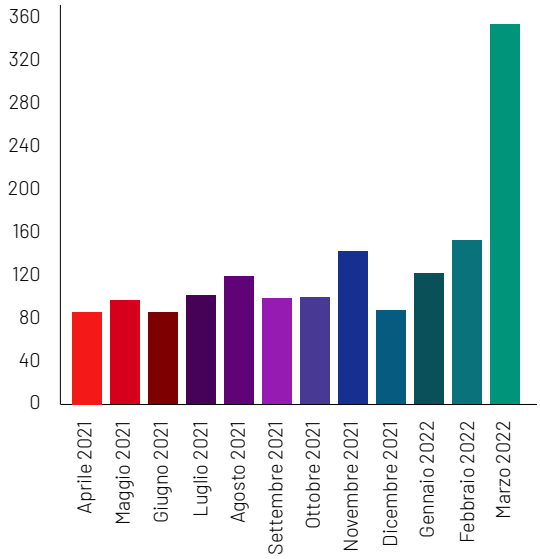

Figura 6. E-mail di phishing identificate contenenti parole chiave specifiche di OT (1° aprile 2021 - 31 marzo 2022).

Dal 1° aprile 2021 al 31 marzo 2022, Mandiant ha osservato oltre 150 domini dannosi con contenuti legati alla produzione industriale e di infrastrutture critiche. Malware come NANOCORE, FORMBOOK, LOKIBOT e VIDAR sono stati identificati nella maggior parte di questi siti Web.

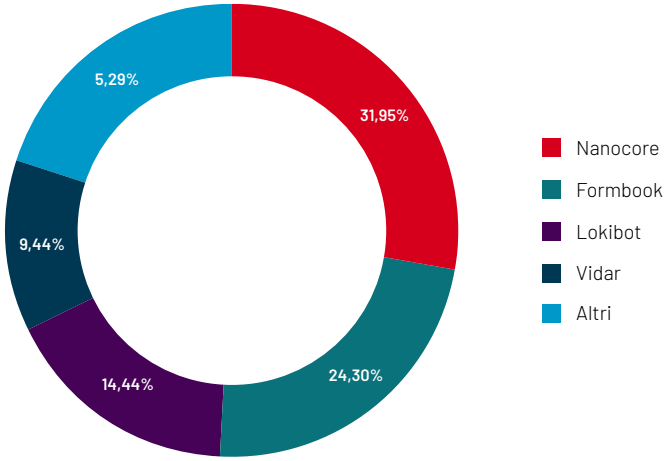

Figura 7. Distribuzione del malware identificato nei domini dannosi con contenuti legati al settore OT (1° aprile 2021 - 31 marzo 2022).

Il valore delle informazioni elaborate sulle vulnerabilità OT

Le prime consulenze sulla vulnerabilità OT sono state rilasciate oltre 10 anni fa. Da allora, gli sforzi per coordinare la comunicazione delle vulnerabilità nei dispositivi OT tra gli enti industriali e governativi sono migliorati e Mandiant continua a registrare un aumento costante del numero di divulgazioni di vulnerabilità. Per comprendere meglio questi dati, Mandiant analizza periodicamente le tendenze e raccoglie dettagli cronologici sui moduli di exploit progettati per sfruttare le vulnerabilità OT.

Dal 1° aprile 2021 al 31 marzo 2022, Mandiant ha monitorato oltre 490 avvisi relativi a vulnerabilità in dispositivi OT o medici di oltre 100 fornitori. Gli avvisi contenevano informazioni su 1.187 vulnerabilità uniche e 196 di esse hanno ricevuto un punteggio di rischio critico. I tipi di vulnerabilità più comunemente osservati sono stati:

- CWE-787: SCRITTURA FUORI DAI LIMITI DELLA MACCHINA
- CWE-125: LETTURA FUORI DAI LIMITI DELLA MACCHINA
- CWE-20: IMPROPER INPUT VALIDATION
- CWE-79: NEUTRALIZZAZIONE IMPROPRIA DELL'INPUT DURANTE LA GENERAZIONE DELLA PAGINA WEB (SCRIPTING CROSS-SITE)
- CWE-121: OVERFLOW DEL BUFFER BASATO SU STACK

Mandiant ha rilevato centinaia di moduli di exploit specifici per il settore OT[16] nelle piattaforme di sicurezza più diffuse. L'accesso a questi strumenti riduce la barriera che impedisce a diversi aggressori di sviluppare competenze o schemi di attacco personalizzati per colpire l'OT. Ad aprile 2022, Mandiant aveva monitorato i moduli di exploit relativi a più di 530 vulnerabilità e il 73% di essi era legato a vulnerabilità del giorno zero.

16. Mandiant (23 marzo 2020). Monitoring ICS Cyber Operation Tools and Software Exploit Modules To Anticipate Future Threats.

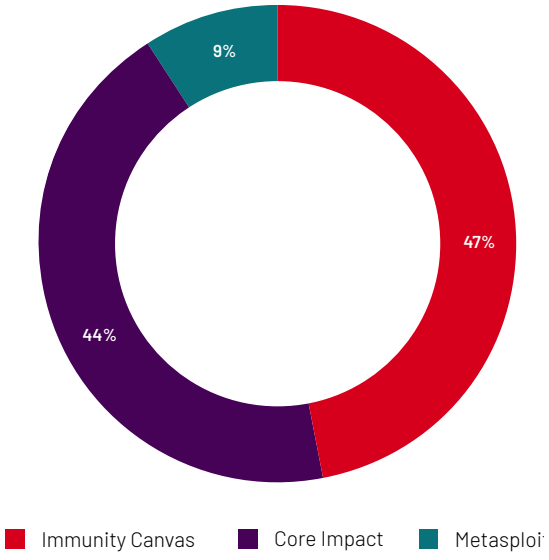

Figura 8. Distribuzione cronologica dei moduli di exploit OT per piattaforma fino ad aprile 2022.

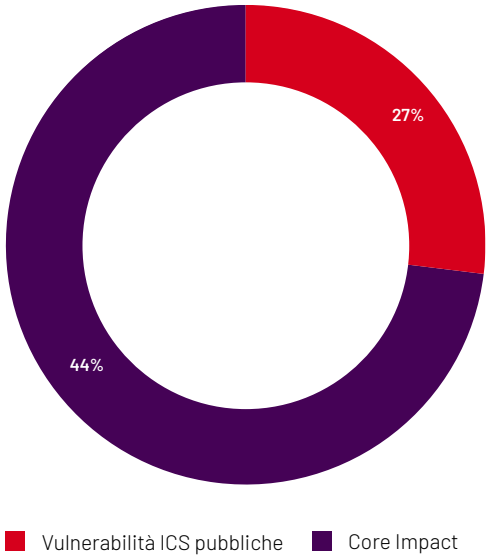

Figura 9. Distribuzione cronologica delle vulnerabilità del giorno zero rispetto alle vulnerabilità OT note nei moduli di exploit fino ad aprile 2022.

Sommario

La visibilità delle minacce Mandiant deriva da una serie di fonti, tra cui:

- Analisi contestuale e tecnica degli eventi d'impatto sulla base dei dati acquisiti dalle attività di risposta agli incidenti
- Raccomandazioni per i difensori basate su una valutazione dell'efficacia della sicurezza dei sistemi ICS rispetto ai principali rischi per le organizzazioni industriali
- Raccolta di dati da parte della rete globale di ricercatori, con un'ampia visibilità sull'attività nei forum online
- Analisi delle minacce si basa sul filtraggio del rumore dei dati presenti nei grandi archivi di intelligence incentrati sull'IT
- Esplorazione del panorama delle minacce e definizione delle tendenze basate sull'analisi dei dati acquisiti da set di dati pubblici, privati e di proprietà di Mandiant

L'insieme di questa ampia visibilità ha permesso a Mandiant di esplorare diverse sfaccettature del panorama delle minacce OT e di acquisire una visione olistica. Le diverse modalità di raccolta dei dati permettono all'azienda di non concentrarsi eccessivamente sugli incidenti OT di alto profilo una volta che si verificano, ma di osservare l'attività degli aggressori molto prima nel ciclo di vita dell'attacco. I dati dimostrano che un attento filtraggio e l'analisi dei dati provenienti dalle minacce nelle reti aziendali possono aiutare i difensori a prevenire futuri attacchi alle reti OT e a rimanere un passo avanti agli aggressori.

Due diligence tecnica per fusioni e acquisizioni

Nei 12 mesi precedenti l'aprile 2022, Mandiant ha completato oltre 240 valutazioni di compromissione su quasi un milione di endpoint. Le valutazioni di compromissione spesso forniscono informazioni per le decisioni pre-acquisizione durante la fase di due diligence di fusioni e acquisizioni e possono anche influenzare le strategie di integrazione tra le aziende coinvolte in fusioni e acquisizioni.

Quando intraprende una valutazione, Mandiant di solito esamina l'ambiente alla ricerca di prove di compromissioni attuali o passate e valuta configurazioni tecniche e controlli specifici. Le metodologie di audit vengono combinate con valutazioni tecniche per garantire l'identificazione di eventuali costi necessari per risolvere le lacune della sicurezza informatica o per aderire a leggi e regolamenti, riducendo il rischio della transazione.

Le valutazioni di compromissione scoprono le lacune della sicurezza

In un caso, Mandiant ha condotto una valutazione di compromissione per un'organizzazione che stava cedendo una singola unità aziendale (SBU) che veniva acquisita da una terza parte. Come parte della sua due diligence, la terza parte ha richiesto un'analisi tecnica dell'unità aziendale per determinare se vi fossero prove di compromissioni in corso o passate o debolezze in controlli di sicurezza specifici. I risultati o le carenze in entrambi gli aspetti potevano avere un impatto sul ritmo e sulla strategia di integrazione della SBU da parte della terza parte.

Mandiant ha condotto la valutazione in un ambiente con Windows. Un'analisi successiva ha rivelato le prove di un precedente evento ransomware. Mentre l'organizzazione era a conoscenza dell'incidente ransomware, Mandiant ha identificato binari residui e backdoor che rimanevano da un tentativo incompleto di correzione.

Mandiant ha inoltre individuato diverse backdoor persistenti che eseguivano il beaconing a server di comando e controllo (C2) non correlati all'attività ransomware. L'analisi dei sistemi che hanno subito l'impatto ha indicato che un aggressore aveva installato le backdoor da sistemi dell'organizzazione più ampia e al di fuori dell'ambito dell'SBU. Tuttavia, l'organizzazione aveva una rete piatta. L'intelligence sulle minacce di Mandiant ha associato le backdoor a un aggressore finanziarie (FIN11) noto per rubare dati e successivamente distribuire ransomware.

Valutando i controlli di sicurezza, Mandiant ha individuato carenze nelle configurazioni degli endpoint e dei domini, nella registrazione dei sistemi, nelle patch e nella pulizia dell'ambiente.

Affrontare i rischi in modo proattivo

Se il cliente non avesse effettuato la valutazione, la terza parte acquirente potrebbe aver collegato le reti interne, esponendo potenzialmente la propria organizzazione ai rischi dell'ambiente SBU.

La terza parte acquirente ha utilizzato i risultati della valutazione per completare un'ulteriore analisi di risposta agli incidenti dell'ambiente per determinare se i dati fossero stati esposti in precedenza. Ha inoltre modificato la propria strategia di integrazione per implementare nuove postazioni di lavoro per gli utenti, migrare i dati su nuovi server e accelerare la migrazione di specifiche applicazioni aziendali verso soluzioni cloud software as a service (SaaS). Queste strategie erano volte a ridurre i rischi per gli ambienti e i dati di entrambe le aziende. Il cliente è stato anche in grado di evitare danni alla reputazione e ulteriori costi, notificando tempestivamente alle parti interessate qualsiasi furto di proprietà intellettuale o di dati.

Protezione degli eventi sociali mentre tutto il mondo sta guardando

I vertici geopolitici globali, le elezioni e gli eventi sportivi sono alcuni degli eventi internazionali, nazionali e regionali a più alta visibilità. Presentano inoltre sfide di sicurezza informatica uniche per quanto riguarda le infrastrutture critiche di supporto e le catene di approvvigionamento. Questi eventi sociali possono durare da un solo giorno a diverse settimane o mesi, richiedendo capacità variabili e di alimentazione aggiuntiva.

Mandiant ha sviluppato un approccio alla sicurezza consigliato e sfaccettato, basato sull'impegno in questo tipo di eventi. Per difendersi dalle minacce informatiche che prendono di mira gli eventi sociali sono necessarie difese attive informate mediante intelligence. Le organizzazioni che gestiscono questi eventi richiedono capacità di programmi di sicurezza strategici e soluzioni tecniche specifiche per rafforzare e migliorare il loro assetto di sicurezza prima di un evento e per supportare le operazioni durante lo stesso. Fornire capacità informatiche resilienti in tempi ristretti, sotto l'intensa attenzione e il controllo dell'opinione pubblica, è una sfida importante che richiede attenzione e investimenti per una corretta pianificazione e attuazione.

Le difese informatiche efficaci per la protezione di eventi importanti si basano su tre fasi:

- Preparazione, rafforzamento ed esercitazione (capire l'ambiente)
- Test, monitoraggio e difesa (anticipare le minacce)
- Risposta, contenimento e correzione (imporre costi e sopravvivere agli attacchi)

Ogni fase riceve informazioni dall'intelligence ed è abbinata a livelli di strutturazione per una protezione proattiva. La raccolta e l'osservazione iniziale dell'intelligence dovrebbero fornire una base del panorama delle minacce per supportare le future capacità di rilevamento. L'intelligence deve evidenziare le attività e le capacità dell'orizzonte avversario durante i principali eventi. Questo aiuta a informare costantemente i difensori sulle attività volte a influenzare, interferire o interrompere gli eventi. Le proprietà di intelligence di Mandiant coprono un'ampia gamma di scenari e includono dettagli sulle tattiche avversarie, sulle motivazioni e sull'evoluzione nel tempo. Queste conoscenze aiutano a definire i livelli del quadro di riferimento per ogni fase.

Mandiant si basa su due categorie di raccomandazioni per rafforzare le difese informatiche di un'organizzazione parallelamente alle condizioni di minaccia emergenti.[17] Le raccomandazioni di rafforzamento e preparazione si concentrano su attività proattive e strategiche, mentre le raccomandazioni operative identificano quali cambiamenti funzionali possono essere adottati per migliorare l'assetto di sicurezza in ogni fase.

17. Mandiant (aprile 2022). A Tiered Framework for Cyber Threat Levels.

Preparazione, rafforzamento ed esercitazione

Questa fase si svolge prima di un evento importante e il suo scopo è quello di proteggere e rafforzare la sicurezza in modo proattivo. La finalità è allineare le difese informatiche dell'ambiente di un'organizzazione alle migliori prassi e agli standard attuali e di supportarne la revisione. L'ambiente delle minacce deve essere definito correttamente in termini di potenziali azioni e motivazioni avversarie. Questa fase è progettata per garantire tre risultati chiave per la difesa informatica attiva: funzioni di base, visibilità e convalida.

Preparazione

- Implementare una capacità di rilevamento e risposta gestita per monitorare e analizzare gli avvisi, andare a caccia di aggressori in modo proattivo e contenere e correggere le minacce.
- Creare casi d'uso e avvisi per le vulnerabilità emergenti e attualmente sfruttate, nonché per le minacce attuali e imminenti, basandosi sul panorama delle minacce e utilizzando informazioni aggiornate e reali.
- Monitorare i social media, i blog, i forum, i siti di notizie e le app di chat per individuare i vettori di minacce e le campagne di disinformazione.
- Implementare le tecnologie di rilevamento degli endpoint e della rete in tutto l'ambiente e l'autenticazione a più fattori su tutti gli account e i servizi rivolti all'esterno.
- Applicare i dati di risposta agli incidenti e i processi, le raccolte e i requisiti tecnologici per accelerare il contenimento e la correzione.
- Assicurare una registrazione olistica e centralizzata su tutte le piattaforme, le reti e gli endpoint.
- Coordinarsi con le agenzie nazionali competenti per ottenere e contribuire alle relative informazioni.
- Ingaggiare una società di consulenza per la risposta agli incidenti per gestire preventivamente gli accordi sui livelli di servizio, i termini e le condizioni e i finanziamenti in caso di violazione.

Rafforzamento

- Eseguire una valutazione della compromissione per garantire la sicurezza e l'integrità dell'ambiente e dei dati da proteggere, in base agli scenari avversari più probabili e più pericolosi.
- Identificare e rinforzare le risorse e i percorsi verso l'ambiente esterno.
- Mantenere un inventario di tutte le risorse sul dominio e sulla rete e far sì che tali risorse vengano regolarmente scansionate per individuare le vulnerabilità e renderle più resistenti.
- Convalidare l'efficacia dei controlli.

Rafforzamento

- Designare un team di risposta alle crisi con ruoli e responsabilità chiare per affrontare i sospetti incidenti di sicurezza informatica; garantire il supporto organizzativo, esecutivo e di comunicazione.
- Testare le procedure di backup per garantire che i dati critici possano essere ripristinati rapidamente e che le funzioni aziendali critiche possano rimanere disponibili in caso di incidente.
- Condurre un'esercitazione tabletop allineata al panorama delle minacce per i grandi eventi per garantire che tutti i partecipanti comprendano i loro ruoli durante un incidente, in base agli scenari precedentemente sviluppati.

Test, monitoraggio e difesa

In questa fase, l'evento principale è iniziato e il rischio di attacchi informatici distruttivi o dirompenti è probabile. Si raccomanda di assumere posizioni elevate di preparazione alla difesa attiva. Le priorità devono includere la convalida continua dei controlli di sicurezza e la difesa delle risorse critiche. Questa fase si concentra sull'inibizione dell'accesso che un avversario deve sfruttare per raggiungere il suo obiettivo. Aumentando le operazioni di ricerca delle minacce si può aumentare la sicurezza che un avversario non mantenga l'accesso alla rete e all'infrastruttura dell'organizzazione. Mandiant può basare tutte le azioni di questa fase sulle attività avversarie conosciute e previste, utilizzando il malware, le tattiche, le tecniche e le procedure degli attaccanti e i fattori motivanti. Questa fase fornisce tre risultati per la difesa informatica attiva: convalida, integrità e vantaggio decisionale.

Test

- Condurre esercitazioni di test di penetrazione ad hoc su tutte le risorse rivolte all'esterno.
- Verificare la capacità del team interno e della tecnologia di rilevamento, prevenzione e risposta.
- Verificare i tempi di reazione del team di risposta agli incidenti contro metodi avversari reali.
- Convalidare continuamente l'efficacia dei controlli di sicurezza informatica.

Monitoraggio

- Stabilire una situation room per centralizzare le informazioni e le comunicazioni delle operazioni, dell'intelligence e dell'organizzazione esterna.
- Monitorare, analizzare e riportare continuamente dati e analisi rilevanti provenienti da fonti di intelligence.
- Eseguire una caccia e un monitoraggio più intensivi per i comportamenti privi di indicatori; supporre che gli attacchi siano in corso e che i controlli tecnici abbiano tralasciato qualcosa.
- Convalidare continuamente l'efficacia dei controlli di sicurezza rispetto ai comportamenti di attacco attivi.
- Limitare le comunicazioni in uscita sui sistemi critici.

Protezione

- Concentrarsi sulla protezione delle risorse critiche: quelle identificate dall'organizzazione target e quelle che potrebbero essere identificate da un avversario.
- Proteggere infrastrutture specifiche di alto valore.
- Limitare l'architettura di rete per limitare o eliminare l'accesso degli avversari ai sistemi critici.
- Eseguire il backup delle risorse critiche.

Risposta, contenimento e correzione

Durante i grandi eventi, la copertura dei media nazionali, internazionali e dei social network è spesso parallela all'attività in tempo reale. Un'ampia intelligence sulle tattiche, le tecniche e le procedure esistenti ed emergenti degli aggressori consente una risposta efficace ed efficiente agli incidenti. I servizi di risposta agli incidenti devono avere la capacità di rispondere, contenere e correggere gli incidenti critici di sicurezza con velocità, ampiezza ed efficienza. Ciò significa utilizzare l'intelligence per stabilire la resilienza in un ambiente di minaccia reale.

La valutazione dei sistemi, delle applicazioni e dell'esposizione alle informazioni che subiscono l'impatto è essenziale per implementare i piani di comunicazione, di crisi e di risposta appropriati. Una risposta efficace agli incidenti e alle violazioni va oltre le indagini tecniche, il contenimento e il recupero e comprende la comunicazione con i dirigenti e la gestione della crisi. La gestione delle crisi include considerazioni legali, normative e di pubbliche relazioni. La criticità di risolvere rapidamente gli incidenti e di garantire la continuità è fondamentale. A tal fine è necessario prendere in considerazione il punto di vista di un potenziale avversario sulla situazione. Prepararsi a un incidente da un solo punto di vista, senza ricorrere all'esperienza reale e ai dati noti sulle minacce, risolve solo metà dell'equazione.

I piani di de-escalation sono spesso più importanti dei piani di escalation. Tutti i difensori devono comunicare e comportarsi in modo ponderato, intenzionale e aperto. Le strategie di contenimento e correzione basate sulle azioni dell'aggressore devono essere implementate per eliminare l'accesso dell'aggressore e migliorare la sicurezza dell'ambiente, così da prevenire o limitare i danni potenziali.

Dopo l'evento principale, un report post-azione dovrebbe descrivere i successi, le sfide e le raccomandazioni.

Questa fase prevede tre risultati per la difesa informatica attiva: risposta, recupero e continuità.

Le sfide della sicurezza informatica che dobbiamo affrontare oggi sono troppo grandi per essere affrontate da soli e la maturità e la capacità delle operazioni di difesa informatica necessarie richiedono un'attenzione e un investimento significativi e sostenuti. Queste sfide si acuiscono ancora di più durante i grandi eventi. La protezione di questi richiede alle organizzazioni di fornire una difesa informatica rapida e adattabile in condizioni di pressione e costrizione uniche. Una strategia e un programma informatici preparati e messi in pratica aiutano a garantire un risultato favorevole per i padroni di casa, i partecipanti e le altre parti interessate.

Per saperne di più, visita il sito www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
Stati Uniti d'America
+1.703.935.1700
+1.833.3MANDIANT (362.6342)
info@mandiant.com

Informazioni su Mandiant

Fin dal 2004, Mandiant® è un partner affidabile di aziende consapevoli della sicurezza. Oggi, le informazioni sulle minacce e l'esperienza di Mandiant, leader del settore, sono alla base di soluzioni dinamiche che aiutano le organizzazioni a sviluppare programmi più efficaci e a infondere fiducia nella loro preparazione informatica.

MANDIANT