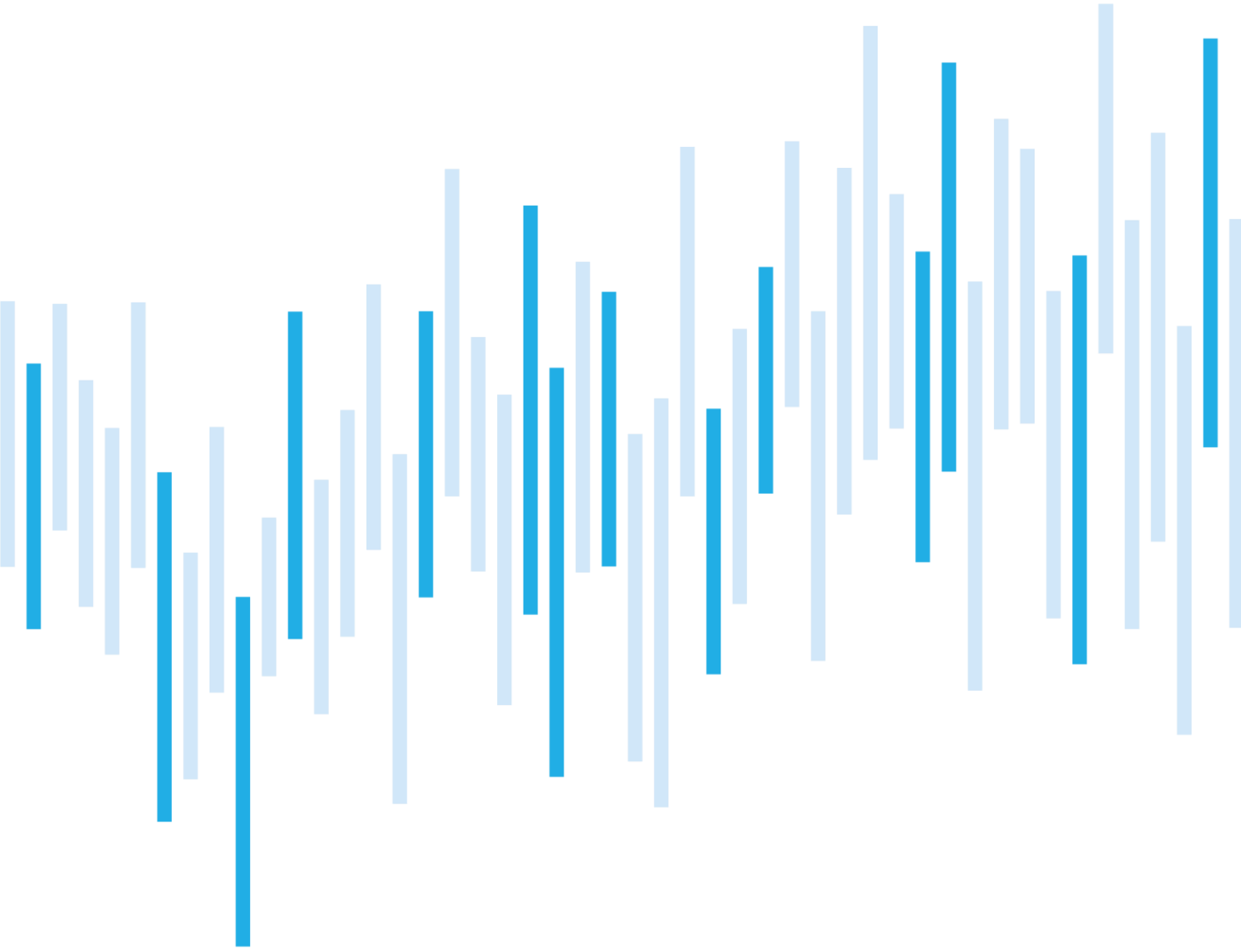
Kybernetické incidenty pohledem NÚKIB

DUBEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Po předchozím rekordním měsíci se počet kybernetických incidentů, které NÚKIB v dubnu řešil, vrátil do průměrných hodnot. Incidentům opět dominovaly případy, ve kterých došlo k narušení dostupnosti služeb. Tentokrát ale nedostupnost nebyla způsobena jen DDoS útoky, v mnoha případech se jednalo o technickou chybu.

V dubnu pokračoval trend intenzivních phishingových kampaní proti strategickým vládním cílům v zemích NATO, včetně ČR. Tento trend nastartovala ruská agrese na Ukrajině, která zvýšila zájem státních aktérů o strategické informace jejich protivníků. V zemích NATO se tak v posledním roce zrychlilo nejen tempo ruských kyberšpionážních útoků, ale také čínských.

Jejich terčem se staly i české diplomatické cíle. Jedná se o kampaň, kterou společnost ESET spojuje se skupinou Mustang Panda. Skupina v kampani použila nový malware MQsTTang. Neobvyklý je na něm především způsob, kterým komunikuje se svým řídicím serverem. Komunikace totiž probíhá přes protokol MQTT, který se využívá pro zařízení internetu věcí (IoT). Žádný veřejně známý malware dosud protokol MQTT nevyužíval. Kampaň a v ní použitou novou techniku blíže popisujeme v posledních dvou kapitolách.

Obsah

Počet kybernetických incidentů nahlášených NÚKIB

Závažnost řešených kybernetických incidentů

Klasifikace incidentů nahlášených NÚKIB

Trendy v kybernetické bezpečnosti za duben pohledem NÚKIB

Technika měsíce: Application Layer Protocol

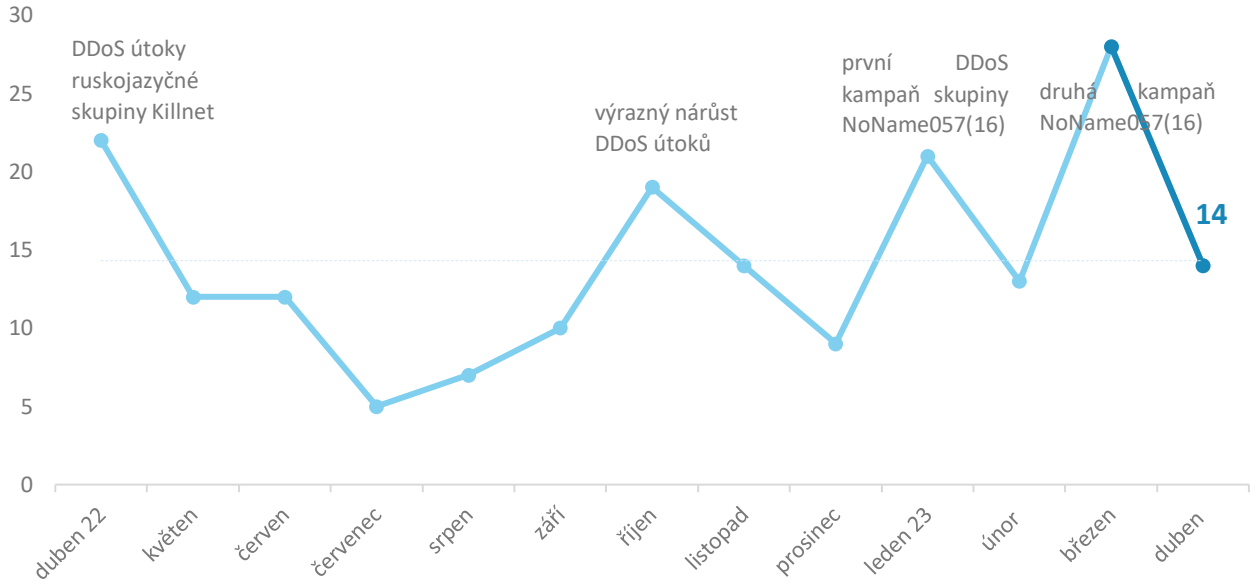
Zaměřeno na hrozbu: Další phishingové kampaně proti českým diplomatickým cílům

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz

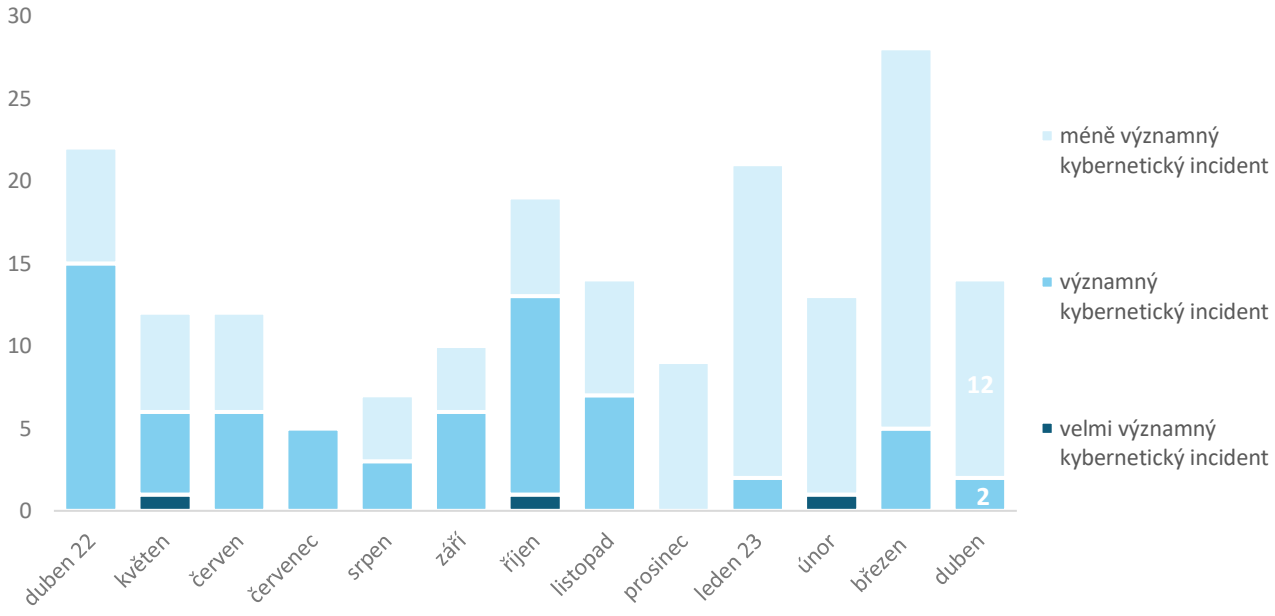
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

NÚKIB v dubnu evidoval 14 kybernetických incidentů. Po předchozím rekordním měsíci se počet incidentů vrátil k průměrným hodnotám posledního roku.[1]



Závažnost řešených kybernetických incidentů[2]

Stejně jako v několika posledních měsících neměla většina kybernetických incidentů závažné důsledky, které by výrazněji ovlivnily chod napadených organizací, a NÚKIB je proto eviduje jako méně významné.



[1] Pět incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývajících devět incidentů nahlásily neregulované subjekty.

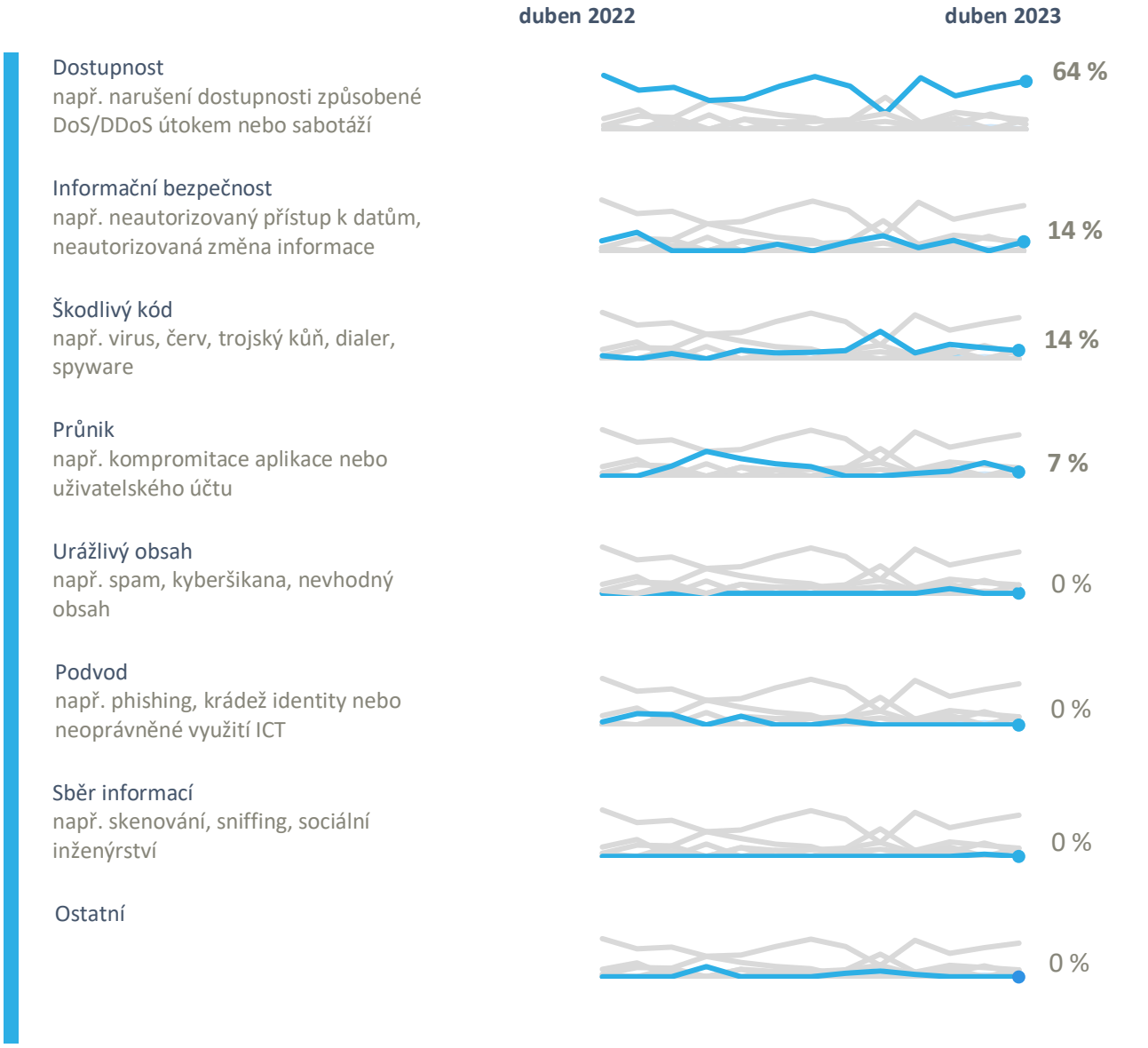
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

V dubnu pokračoval trend posledního roku, kdy incidentům dominovalo narušení dostupnosti služeb. NÚKIB takto klasifikoval téměř dvě třetiny incidentů. Na rozdíl od přechozího měsíce ale příčinou nebyly pouze DDoS útoky, ale z velké části technické chyby. Výpadek služeb způsobený chybou nahlásilo NÚKIB pět organizací.

Vedle dostupnosti NÚKIB řešil také incidenty v těchto kategoriích:

- Dva incidenty, při nichž útočník po kompromitaci změnil údaje na webových stránkách oběti, NÚKIB klasifikoval jako informační bezpečnost;
- Dva incidenty způsobené ransomwarem NÚKIB evidoval jako škodlivý kód,
- A v posledním případě neznámí útočníci kompromitovali e-mailovou schránku zaměstnance soukromé organizace a následně z ní rozesílali spamy na další adresy.



[3] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu)

Trendy v kybernetické bezpečnosti za duben pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Pokračuje trend intenzivních phishingových kampaní proti strategickým vladním cílům v zemích NATO, včetně ČR. Tento trend nastartovala ruská agrese na Ukrajině, která zvýšila zájem státních aktérů o strategické informace jejich protivníků. Podle veřejně dostupných informací se v zemích NATO v posledním roce navýšilo nejen tempo ruských kyberšpionážních útoků, ale také čínských.

Malware

V jedné z nedávných phishingových kampaní, kterou NÚKIB analyzoval a kterou popisujeme v poslední kapitole, se objevil nový malware MQsTTang. Útočníci ho používají jako backdoor a zajímavý je na něm především způsob, kterým komunikuje se svým řídicím serverem. Komunikace probíhá přes protokol MQTT, který se využívá pro zařízení internetu věcí (IoT). Žádný veřejně známý malware dosud protokol MQTT nevyužíval. Více informací k této technice naleznete v následující kapitole.

Zranitelnosti

V dubnu se neobjevila žádná nová závažná zranitelnost, u které bychom očekávali plošné zneužívaní a která by mohla být zneužívána napříč povinnými osobami NÚKIB.

Ransomware

NÚKIB evidoval dva případy ransomwarových útoků, oba proti malým a středním podnikům. Za jedním z incidentů stál LockBit 2.0, ransomware z jedné z nejvíce aktivních „ransomwarových rodin“ v ČR.

Počtem a charakterem obětí byly dubnové ransomwarové útoky podobné předešlým 12 měsícům. Útoky, které v posledním roce NÚKIB eviduje, nejčastěji zasahují menší podniky nebo základní a střední školy.

Útoky na dostupnost

V dubnu pokračovaly dozvuky březnové vlny hacktivistických DDoS útoků proti českým cílům. Jejich intenzita byla ale oproti předchozímu měsíci nižší a počet DDoS útoků, které NÚKIB v této souvislosti řešil, poklesl na třetinu. Útočníci se zaměřili především na organizace z dopravního sektoru.

OT – operační technologie

Ukrajinský CERT (CERT-UA) v dubnu informoval o incidentu, kdy si zaměstnanec energetické společnosti stáhnul z Torrent sítě pirátský Microsoft Office 2019. Následkem toho došlo ke kompromitaci počítače pomocí malware DarkCrystal a DWAgent. Tyto dvě aplikace poskytovaly neoprávněný přístup do sítě společnosti po dobu dvou měsíců. Více informací na CERT-UA.

[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Technika měsíce: Application Layer Protocol

Útočníci v phishingové kampani, kterou popisujeme v následující kapitole, použili neobvyklý způsob komunikace mezi jejich řídícím serverem (C2 serverem) a kompromitovanou stanicí oběti. Komunikaci posílali skrze protokol MQTT, který se používá pro správu IoT zařízení. To je odlišuje od dalších aktérů. Obecně tato technika v MITRE matici spadá pod Application Layer Protocol.

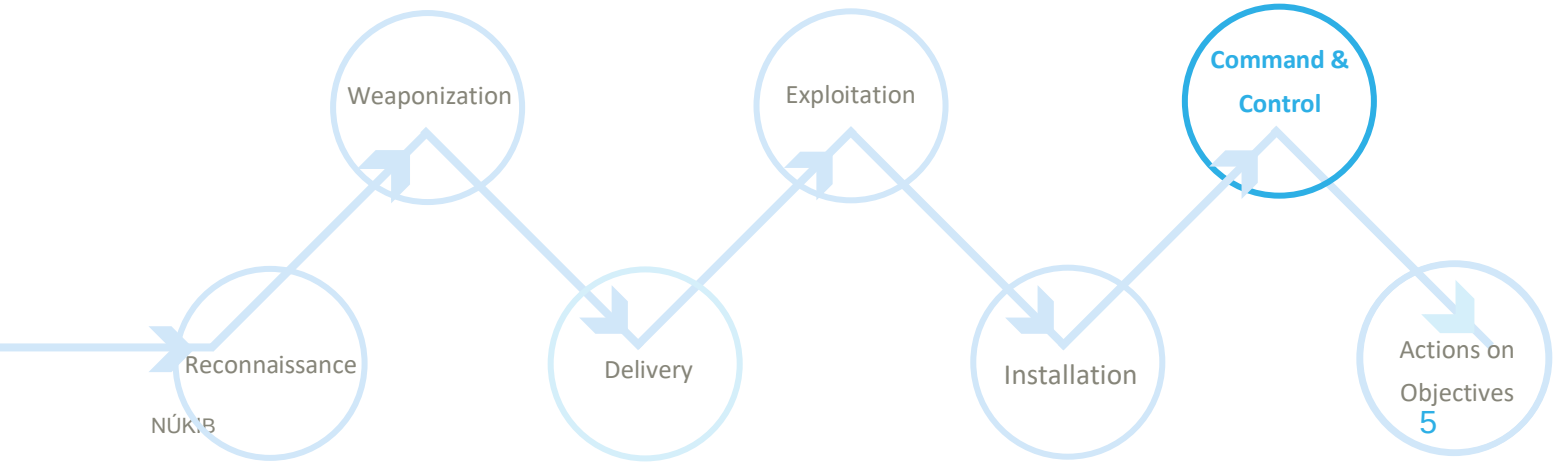
Application Layer Protocol: Ve chvíli, kdy útočníci proniknou do sítě své oběti a nainstalují do ní backdoor, potřebují, aby začal komunikovat s jejich infrastrukturou a oni přes něj mohli přistupovat do sítě oběti a podnikat v ní další kroky. Aby nedošlo k odhalení jejich útoku, často se snaží škodlivou komunikaci s C2 serverem schovat mezi běžně používané protokoly jako například HTTP/HTTPS, DNS nebo protokoly pro elektronickou poštu (SMTP, POP3). Doufají, že se ve velkém objemu legitimního provozu na těchto protokolech jejich činnost ztratí a tím pádem bude pro obránce hůře detekovatelná.

V námi popisované kampani nicméně útočníci nekomunikovali se svou infrastrukturou pomocí běžně známých protokolů, ale skrze protokol MQTT (port 1883). Tento protokol se používá pro komunikaci zařízení internetu věcí. Z pohledu útočníka má MQTT protokol tu výhodu, že může skrýt svou infrastrukturu za veřejného brokera (centrální prvek, který řídí komunikaci mezi IoT zařízeními). Oběť tak nikdy nekomunikuje přímo s řídicím serverem útočníka, ale se serverem brokera. To činí útočníkovu infrastrukturu hůře viditelnou. Analytici společnosti ESET poznamenávají, že jelikož útočníky využívaný broker je veřejná služba, která má mnoho legitimních uživatelů, je nepravděpodobné, že bude odstraněna.

MITRE ID: T1071

Mitigace: Obtížnost mitigace této techniky závisí na frekvenci MQTT protokolu v síťovém provozu organizací. Některé organizace, které aktivně využívají IoT zařízení, jako např. průmysl, energetika nebo zdravotnictví, mohou mít MQTT protokol ve svém síťovém provozu velmi často. Nicméně, v jiných organizacích, které nemají rozsáhlé nasazení IoT zařízení, se MQTT protokol nemusí v síťovém provozu vyskytovat často nebo vůbec. Obránci sítě pak mohou provoz MQTT protokolu snáze monitorovat a filtrovat, popřípadě zcela zakázat. Dále doporučuje segmentaci sítě a případná IoT zařízení, jako např. tiskárny, umístit do oddělené VLAN.

Znázornění Application Layer Protocol v kill chainu ukazujícím, v jaké fázi útoku kybernetičtí aktéři techniku používají:



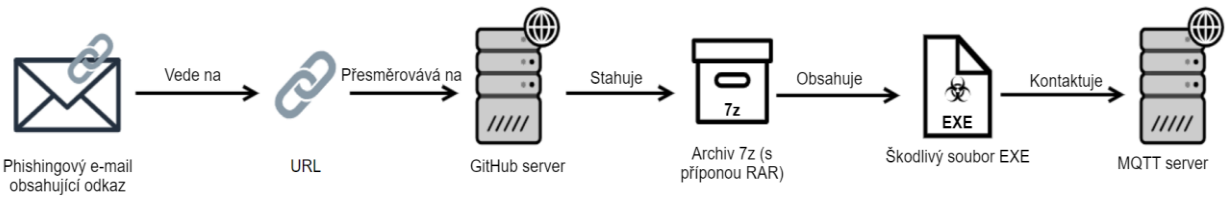
Zaměřeno na hrozbu: Další phishingové kampaně proti českým diplomatickým cílům

České diplomatické cíle se v minulých měsících opět dostaly do hledáčku kyberšpionážních aktérů. Jedná se o kampaň, kterou ESET spojuje s čínskou skupinou Mustang Panda. Skupina je typická především svým zaměřením na diplomatické organizace. Od začátku ruské agrese na Ukrajině zrychlila tempo svých útoků a přesunula většinu své pozornosti na evropské subjekty. Zde popisovaná kampaň nemířila jen na ČR, ale na více zemí NATO a EU.

Na této kampani je zajímavý nový malware MQsTTang, který skupina ve svých útocích použila. Útočníci ho využívají jako backdoor a neobvyklý je na něm především způsob, kterým komunikuje se svým řídicím serverem. Komunikace probíhá přes protokol MQTT, který se využívá pro zařízení internetu věcí (IoT). Žádný veřejně známý malware dosud protokol MQTT nevyužíval.

Na základě jednoho z phishingových e-mailů, který NÚKIB získal, identifikoval, jak útoky nedávné kampaně probíhaly:

Útok začal phishingovým e-mailem s diplomatickou tématikou a škodlivým odkazem. Po rozkliknutí odkazu se oběť dostala na URL, odkud byla dále přesměrována na útočníkovu stránku na platformě GitHub. Na tu útočníci umístili archiv, který si oběť stáhla k sobě do počítače. Archiv po svém rozbalení obsahoval soubor EXE, což je malware MQsTTang. Pokud oběť soubor spustila, začal malware komunikovat se svým řídicím serverem pomocí MQTT protokolu (viz předchozí kapitola). V dalších krocích si pak útočníci vytvořili v síti oběti persistenci a začali do ní stahovat další nástroje pro kyberšpionážní účely.



Přestože čínské APT skupiny míří na evropské organizace dlouhodobě, invaze na Ukrajinu dala jejich útokům nový impuls. Vzhledem ke zvýšené aktivitě čínských skupin, kterou popisují bezpečnostní společnosti, je téměř jisté (90–100 %), že po dobu trvání války bude Mustang Panda i nadále cílit na evropské organizace, ze kterých se bude snažit získat strategické informace. A jak ukazuje její poslední kampaň, je také pravděpodobné (55–70 %), že skupina své útoky bude dále vylepšovat a nasazovat v nich nové techniky a nástroje.

Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit/Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP: CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.