APT40 Зөвлөмж

БНХАУ-ын Төрийн Аюулгүй Байдлын Яам (MSS)-ын тагнуулын аргачлалын хэрэгжилт

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

ГАРЧИГ

Тойм

Ерөнхий мэдээлэл

Мэдээлэл технологийн аюулгүй байдлын энэхүү зөвлөмжийг дараах байгууллагууд хамтран боловсруулсан болно. Үүнд: Австралийн Холбооны Дохиоллын Газрын (ASD) дэргэдэх Австралийн Цахим Аюулгүй Байдлын Төв (ACSC), АНУ-ын Цахим аюулгүй байдал, Дэд бүтцийн аюулгүй байдлын агентлаг (CISA), Үндэсний Аюулгүй Байдлын Агентлаг (NSA), Холбооны Мөрдөх Товчоо (FBI), Их Британийн Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC-UK), Канадын Цахим Аюулгүй Байдлын Төв (CCCS), Шинэ Зеландын Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC-NZ), Германы Холбооны Тагнуулын Алба (BND) болон Үндсэн хуулийг хамгаалах холбооны газар (BfV), БНСУ-ын Үндэсний Тагнуулын Алба (NIS) болон NIS-ийн харьяа Цахим Аюулгүй Байдлын Үндэсний Төв, Японы Цахим Халдлагад Бэлэн Байдлыг Хангах, Стратеги Боловсруулах Үндэсний Төв (NISC) болон Үндэсний Цагдаагийн Агентлаг (NPA) багтана. Эдгээр байгууллагуудыг цаашид "зохиогч агентлагууд" гэж нэрлэнэ. Энэхүү зөвлөмжид Бүгд Найрамдах Хятад Ард Улсын (БНХАУ) төрийн дэмжлэгтэй цахим бүлэглэл болон тэдгээрийн Австралийн сүлжээнд учруулж буй одоогийн аюулыг тусгасан болно. Энэхүү зөвлөмжийг нийтэлсэн агентлагуудын цахим аюулын талаарх хамтарсан ойлголт болон цахим халдлагын ASD-ийн ACSC-ээс хийсэн хариу арга хэмжээний судалгаанд тулгуурлан бүтээв.

БНХАУ-ын төрөөс дэмжлэг авсан цахим бүлэглэл өмнө нь Австрали, АНУ зэрэг олон улсын байгууллагуудыг чиглэсэн дайралт хийж байсан бөгөөд доорх арга техникүүдийг дэлхий даяар бусад БНХАУ-ын төрийн ивээл дор үйл ажиллагаа явуулдаг цахим бүлэглэлүүд тогтмол ашигладаг. Иймд эдгээр бүлэглэл болон ашиглагдаж буй техник, арга барил нь зохиогч агентлагуудын улс орны сүлжээнд мөн адил аюул учруулж байгаа хэмээн дүгнэж байна.

Зохиогч агентлагууд энэхүү бүлэглэлийг БНХАУ-ын Төрийн Аюулгүй Байдлын Яам (MSS)-ны удирдлага дор хорлон сүйтгэх цахим ажиллагаа явуулдаг гэж дүгнэж байна. Тэдний үйл ажиллагаа, ашиглаж буй арга техник нь салбарын тайлангууд дээрх Kryptonite Panda, GINGHAM TYPHOON, Leviathan, Bronze Mohawk гэх нэрээр бүртгэгдсэн Advanced Persistent Threat буюу APT40 бүлэгтэй ижил байгаа юм. Энэхүү бүлэглэлийг өмнө нь Хайнань мужийн Хайкоу хотод төвтэй бөгөөд Хятадын Төрийн Аюулгүй Байдлын Яамны тус хот дахь салбараас үүрэг, даалгавар авдаг гэж мэдээлж байсан.[2] Дараах зөвлөмжид халдлагын арга техникүүдийг хоёр хохирогчийн сүлжээнд хэрхэн хэрэгжүүлсэнийг харуулах онцлох жишиг судалгааны жишээг өгүүлнэ. Эдгээр жишиг судалгаанууд нь цахим аюулгүй байдлын мэргэжилтнүүдэд өөрсдийн сүлжээг APT40 бүлэглэлийн халдлагаас хамгаалах, халдлагыг илрүүлэх болон сэргээн засварлах үйл ажиллагаанд чухал ач холбогдолтой юм. Сонгогдсон жишиг судалгаанууд нь халдлагад өртсөн байгууллагууд зохих хариу арга хэмжээг авч, дахин халдлагад өртөх эрсдэлийг бууруулсан тохиолдлууд юм. Ийм учраас эдгээр жишээнүүд нь харьцангуй хуучны үйл явдлууд бөгөөд холбогдох байгууллагуудад хамгаалалтын арга хэмжээ авах, хэрэгжүүлэх хангалттай хугацаа байсан гэж үзэж болно.

Үйл ажиллагааны хураангуй

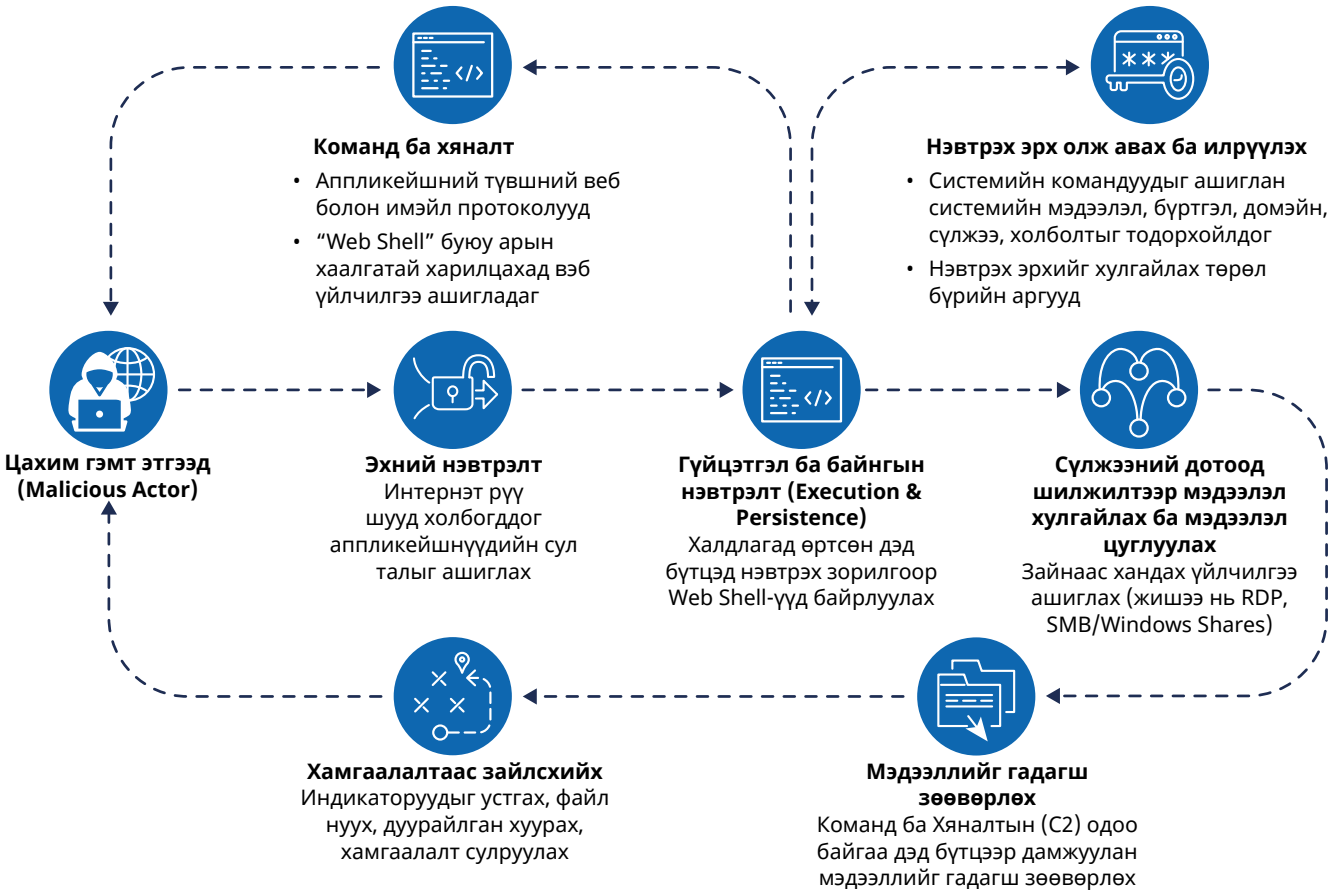
APT40 бүлэглэл Австралийн сүлжээнүүд болон бүс нутгийн төрийн болон хувийн хэвшлийн байгууллагуудын сүлжээг удаа дараа онилж ирсэн бөгөөд тэдний учруулж буй аюул одоог хүртэл үргэлжилсээр байна. Энэхүү зөвлөмжид дурдсан арга барилыг Австралийн сүлжээнүүдэд халдлага хийхэд байнга ашиглаж байгаа нь ажиглагдсан.

Тухайлбал, APT40 бүлэг нь шинэ аюулгүй байдлын сул талыг илрүүлэх туршилтын загварыг (POC) богино хугацаанд боловсруулж, холбогдох сул тал бүхий дэд бүтэцтэй сүлжээнд шууд ашиглан халдах чадвартай. APT40 бүлэг халдлага хийх боломжийг эрэлхийлэн, энэхүү зөвлөмжийг хамтран гаргасан агентлагуудын төрийн мэдлийн сүлжээг болон бусад зорилтот сүлжээнүүдэд тогтмол тандалт хийдэг. Энэхүү тогтмол тандалтаар зорилтот сүлжээнүүдийн хамгаалалтгүй, ашиглалтаас гарсан буюу засвар үйлчилгээ хийгдээгүй төхөөрөмжүүдийг илрүүлж, шуурхай сул талыг ашиглах нөхцөл бүрдүүлдэг. APT40 бүлэг 2017 оноос хойш програм хангамжийн сул талыг ашиглан амжилттай халдлага хийсээр байна.

Энэ бүлэглэл нь Log4J (CVE-2021-44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) болон Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) зэрэг өргөн хэрэглэгддэг програм хангамжуудад шинээр илэрсэн сул талыг маш богино хугацаанд ашиглан халдлага хийдэг. ASD-ийн ACSC болон бусад зохиогч агентлагуудын таамаглаж буйгаар, уг бүлэглэл цаашид ч шинээр олон нийтэд танилцуулах программын сул талыг хэдхэн цаг, өдрийн дотор POC-уудаа (proof-of-concept) ашиглан хурдан хугацаанд халдлага явуулах төлөвтэй байна.

2 АНУ-ын Хууль Зүйн Яам. 2021. Төрийн Аюулгүй Байдлын Яамтай хамтран ажиллаж байсан Хятад улсын дөрвөн иргэнийг халдварт өвчний судалгаанаас эхлээд оюуны өмчийн болон бизнесийн нууц мэдээлэл рүү чиглэсэн олон улсын цахим халдлагын үйл ажиллагаандоролцсон гэх үндэслэлээр буруутган ял оноожээ.

Зураг 1: APT40 үйл ажиллагааны TTP урсгал диаграм



Энэ бүлэглэл нь хэрэглэгчийн оролцоо шаардсан фишинг зэрэг арга техникийг ашиглахаас илүүтэй, ил тод, интернэтэд нээлттэй байрласан эмзэг дэд бүтцэд шууд халдахыг илүүд үздэг. Мөн тэд хууль ёсны нэвтрэх эрх (нууц үг, итгэмжлэл) олж авахыг маш чухалчилдаг ба энэ нь дараагийн олон төрлийн халдлагыг гүйцэтгэх үндэс суурь болдог. APT40 бүлэглэл нь тогтвортой нэвтрэх орчныг бий болгохын тулд ялангуяа халдлагын эхний шатанд тогтмол арын хаалга буюу “web shell”-г ашигладаг (T1505.003). Ерөнхийдөө, анхны нэвтрэлт амжилттай болсны дараа APT40 бүлэг тогтмол нэвтрэхийг зорьдог. Гэвч тогтмол нэвтрэлт (persistence) ихэвчлэн халдлагын эхэн үед явагддаг учраас энэ нь халдлагын цар хүрээ, дараагийн үйлдлүүдээс үл хамааран бараг бүх халдлага дээр илэрдэг.

Онцлох арга барил

APT40 нь өмнө нь Австралийн вебсайтууд руу халдаж, үйл ажиллагаандаа команд ба хяналтын (C2) хост болгон ашиглаж байсан ч, энэ техникээ өөрчилж сайжруулсан байна (T1594).

APT40 бүлэглэл нь сүүлийн үед дэлхий даяар ажиглагдаж буй чиг хандлагыг даган, жижиг оффис/гэрийн хэрэглээний төхөөрөмжүүдийг (SOHO – small-office/home-office devices) үйл ажиллагааны дэд бүтэц болон сүүлчийн дамжуулагч (last-hop redirector) болгон ашиглах болсон бөгөөд энэ нь Австрали дахь халдлагад мөн хамаарна (T1584.008).

Энэхүү арга барил нь зохиогч агентлагуудын хувьд APT40 бүлэглэлийн үйл ажиллагааг илүү нарийвчлан шинжилж, хянах боломжийг бүрдүүлсэн.

Ийм төрлийн SOHO (жижиг оффис/гэрийн хэрэглээний) төхөөрөмжүүд нь ихэвчлэн ашиглалтын хугацаа нь дууссан эсвэл шинэчлэлт хийгдээгүй байдаг тул N-day төрлийн хялбар бай болдог. Нэгэнт халдлагад өртсөн тохиолдолд, эдгээр төхөөрөмжүүд нь хууль ёсны сүлжээний урсгалыг дуурайлгах замаар халдлага эхлүүлэх цэг болж, сүлжээний хамгаалалтын системүүдийг төөрөгдүүлж, илрэхгүй байх нөхцөл бүрдүүлдэг (T1001.003).

Энэ техникийг зөвхөн APT40 биш, БНХАУ-ын төрийн дэмжлэгтэй бусад олон цахим бүлэглэлүүд дэлхий даяар тогтмол ашиглаж байгаа бөгөөд зохиогч агентлагууд энэ аргыг нийтлэг аюул гэж үзэж байна. Нэмэлт мэдээллийг дараах хамтарсан зөвлөмжөөс үзнэ үү: Бүгд Найрамдах Хятад Ард Улсын төрийн дэмжлэгтэй цахим бүлэглэлүүд сүлжээний үйлчилгээ үзүүлэгчид болон төхөөрөмжүүдийг ашиглаж буй талаар болон БНХАУ-ын төрийн дэмжлэгтэй бүлэглэлүүд АНУ-ын стратегийн ач холбогдол бүхий дэд бүтцэд халдан, урт хугацаанд хандалтаа хадгалсан тухай.

APT40 бүлэглэл зарим тохиолдолд худалдан авсан буюу түрээслэсэн дэд бүтцээ хохирогч руу чиглэсэн C2 дэд бүтэц болгон ашигладаг. Гэвч, энэ арга барил нь харьцангуй цөөрөх хандлагатай байна.

Арга хэрэгслүүд

ASD-ийн дэргэдэх ACSC нь доорх мөрдөн шалгалтуудаар илэрсэн хортой файлуудын заримыг олон нийтэд дэлгэж байна. Эдгээр файлуудыг VirusTotal платформд байршуулснаар сүлжээний хамгаалалт болон цахим аюулгүй байдлын мэргэжилтнүүд тухайн аюул заналхийллийг илүү нарийвчлан судалж, үр дүнтэй хамгаалах арга хэмжээг цаг алдалгүй авах боломжтой болсон.

Жишиг судалгаа

ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC) нь уг бүлэглэл хэрхэн өөрсдийн хэрэгсэл, арга барилыг ашигладаг талаар мэдлэг олгох зорилгоор дараах хоёр нэрийг нь нууцалсан судалгаа, мөрдөн шалгалтын тайланг хуваалцаж байна.

MD5	Файлын нэр	Нэмэлт мэдээлэл
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

Жишиг судалгаа 1

Энэхүү тайланг олон нийтэд илүү түгээх үүднээс нэр, байгууллагын мэдээллийг нууцалсан болно. Халдлагад өртсөн байгууллагыг цаашид "байгууллага" гэж нэрлэнэ. Хохирогч байгууллага болон ASD-ийн ACSC-ийн хэрэгжүүлсэн хариу арга хэмжээний аргачлалыг нууцлах зорилгоор зарим нарийн мэдээллийг хассан болно.

Товч хураангуй

Энэхүү тайланд ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC)-ийн 2022 оны долоодугаар сараас есдүгээр сарын хооронд байгууллагын сүлжээнд амжилттай халдсан тохиолдлын мөрдөн шалгалтын үр дүнг тусгасан болно. Мөрдөн шалгалтын энэхүү тайланг байгууллагад хүргүүлсэн бөгөөд илэрсэн халдлагын үйл ажиллагааг нэгтгэн дүгнэж, хамгаалалт, сэргээлтийн зөвлөмжийг хүргэсэн болно. Мөрдөн шалгалтын үр дүнд энэхүү халдлагыг APT40 бүлэглэл үйлдсэн болохыг тогтоосон.

2022 оны наймдугаар сарын дунд үед ASD-ийн ACSC нь тус байгууллагын сүлжээнд APT40 бүлгийн явуулсан сэжигтэй үйл ажиллагааг илрүүлж, үүний талаар мэдэгдсэн. Байгууллагын зөвшөөрлийн дагуу, ACSC нь хариу арга хэмжээний хүрээнд халдлагад өртсөн байж болзошгүй төхөөрөмжүүд дээр хост суурьтай мэдрэгч (host-based sensor) суурилуулсан. Эдгээр сенсоруудын тусламжтайгаар ASD-ийн ACSC-ийн шинжээчдэд нарийвчилсан дижитал шинжилгээ (digital forensics) хийх боломжтой болсон. Мэдээлэл цуглуулах мэдрэгчүүдийн өгөгдөлд үндэслэн, ACSC-ийн шинжээчид халдлагын бүлэглэлийн үйл ажиллагааг амжилттай тодорхойлж, болсон үйл явдлуудын дэлгэрэнгүй цаг хугацааны дарааллыг гаргажээ.

2022 оны 7-8 саруудад ACSC-ийн ACSC дараах гол үйл ажиллагааг илрүүлсэн:

- Хост тандан судалгаа (host enumeration): Халдагч сүлжээний бүтцийн зураглалыг гаргах;
- Арын хаалга (web shell) ашиглалт: Сүлжээнд анхны хандалт үүсгэх ба командыг зайнаас гүйцэтгэх боломж олгодог;
- Бусад хортой хэрэгслийн байршуулалт: Халдлага хийх зорилгоор тусгай програмууд ашиглах.

Шалгалтын явцад тухайн бүлэглэл, их хэмжээний хувийн мэдээлэлд нэвтэрсэн, мөн сүлжээгээр дотоод (lateral movement) шилжилт хийх байдлаар мэдээлэл хулгайлсан (T1021.002) ул мөр , нотолгоонууд илэрсэн. Халдлагын ихэнх хэсгийг бүлэглэл сүлжээнд нэвтрэх олон суваг (access vectors) бий болгосон, сүлжээ нь "flat" буюу хэсэгчлээгүй бүтэцтэй байсан, мөн дур мэдэн файл байршуулж болох хамгаалалтгүй дотооддоо хөгжүүлсэн програм хангамж ашигласан зэрэг нөхцлүүд бүрдсэн байдалтай холбон тайлбарлаж болно. Гадагш зөөвөрлөгдсөн мэдээлэлд бүлэглэлд сүлжээнд нэвтрэх боломж олгосон эрх бүхий баталгаажуулалтын бүртгэлийн мэдээлэл, мөн анхны нэвтрэх суваг хаагдсан тохиолдолд дахин зөвшөөрөлгүй нэвтрэхэд ашиглаж болох сүлжээний бүтцийн мэдээлэл багтаж байв. Хамгийн анх халдлагад өртсөн төхөөрөмжөөс өөр хортой хэрэгсэл илрээгүй боловч тус бүлэг нь хууль ёсны, эрх бүхий бүртгэлийн мэдээлэлд нэвтрэх боломжтой байсан нь цаашид тусгай хэрэгсэл ашиглах шаардлагагүй болгож байв. Мөрдөн шалгалтын үр дүнгээс үзэхэд, уг байгууллага нийтэд ил болсон программ хангамжын сул талд санамсаргүйгээр өртсөн бус, харин APT40 бүлэглэлийн санаатайгаар бай болгосон, зорилтот халдлагын золиос болсон нь тогтоогдсон байна.

Мөрдөн шалгалтын үр дүн

2022 оны наймдугаар сарын дунд үед, ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC) тухайн байгууллагад хандан, долдугаар сараас наймдугаар сар хүртэл тус байгууллагын компьютерийн сүлжээнд улсын санхүүжилттэй хакерын бүлэгтэй холбоотой батлагдсан нэгэн хортой IP хаяг холбогдсон тухай мэдээлсэн. Халдлагад өртсөн төхөөрөмж нь магадгүй жижиг бизнес эсвэл хувь хэрэглэгчид харьяалагддаг байсан байх өндөр магадлалтай.

Наймдугаар сарын сүүл үед, ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC) тухайн байгууллагын сүлжээнд хост дээр суурилсан програм суурилуулсан ба үүний үр дүнд халдлагад өртсөнийг илрүүлж чадсан.

Мөрдлөгийн ажиллагаанд тус болох байсан зарим эд мөрийн баримтууд нь лог бүртгэлийн тохиргоо эсвэл сүлжээний бүтцийн онцлогоос шалтгаалан ашиглах боломжгүй байсан. Гэсэн хэдий ч байгууллагаас боломжтой бүх мэдээллийг бүрэн, шуурхай гаргаж өгсөн нь ASD-ийн ACSC-ийн шинжээчдэд нарийвчилсан дүн шинжилгээ хийх боломж олгож, APT40 бүлгийн сүлжээнд явуулсан үйл ажиллагааны талаар бодит ойлголт авахад чухал хувь нэмэр болсон.

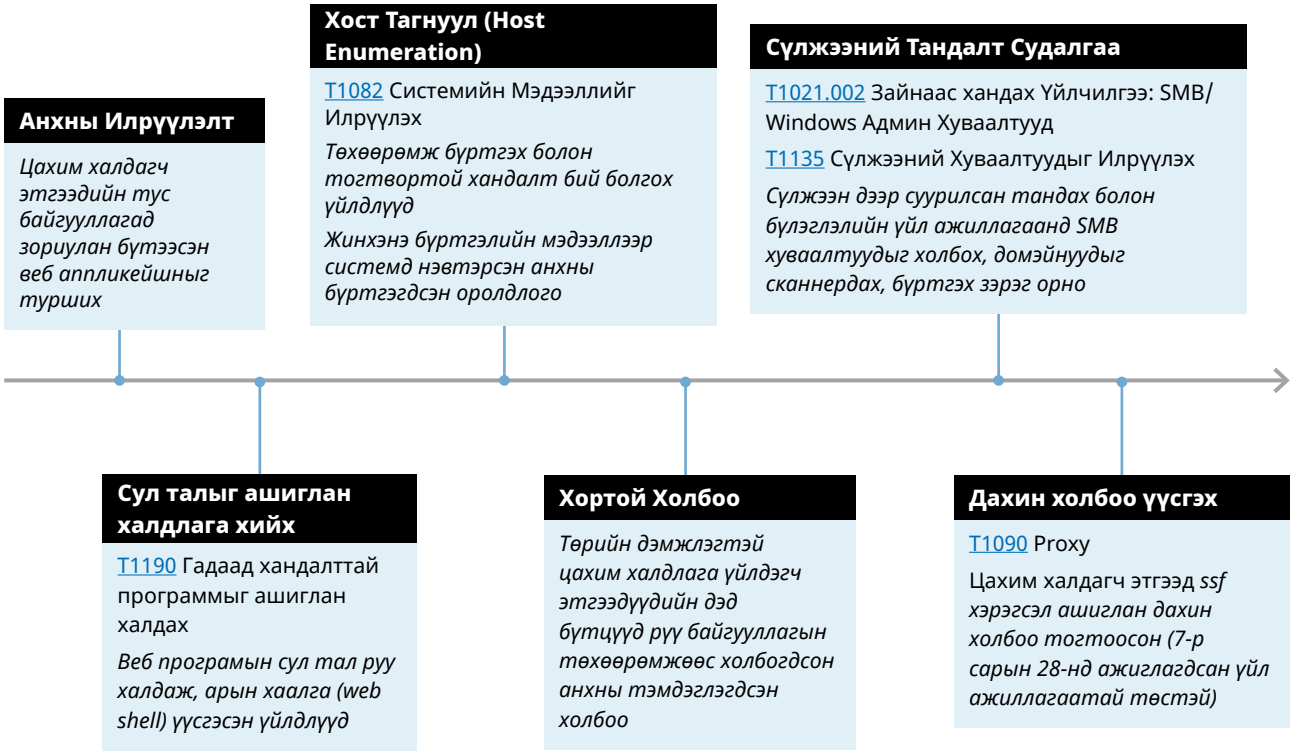
Есдүгээр сард, ASD-ийн ACSC-тэй зөвлөлдсөний дараа, байгууллага анхлан мэдээлэгдсэн сэжигтэй IP хаягийг хар жагсаалтад (denylist) оруулахаар шийдсэн. Аравдугаар сард, байгууллага алдааг засах буюу сэргээх ажиллагаагаа эхлүүлсэн.

Дэлгэрэнгүй

Долоодугаар сараас эхлэн, халдагч этгээдүүд `<webapp>2-ext` дээр ажиллаж байсан тусгайлан боловсруулсан веб програмыг (T1190) шалгаж, ашиглан сүлжээний DMZ (Сүлжээний Хамгаалалт Сул Бүс) хэсэгт байршуулж чадсан. Энэ боломжийг ашиглан тэд тухайн сүлжээ болон ил харагдаж байсан бүх домэйнүүдийг тоолж, зураглал үүсгэсэн. Хулгайлагдсан нэвтрэх эрхүүдийг (T1078.002) ашиглан Active Directory-с (T1018) мэдээлэл хайж, мөн DMZ доторх хэд хэдэн төхөөрөмжөөс файл хуваалцах протоколыг ашиглан (T1039) мэдээллийг гадагш зөөвөрлөжээ. Халдагч этгээд сүлжээний серверээс хүчинтэй сүлжээний нэвтрэх эрх авах зорилгоор Керберос халдлагыг гүйцэтгэсэн (T1558.003). Цахим халдлага үйлдэгч бүлэглэлийн зүгээс DMZ болон дотоод сүлжээний өөр бусад хэсэгт нэвтэрсэн болох нь ажиглагдаагүй.

Цаг хугацааны дараалал

Доорх цаг хугацааны дараалал нь байгууллагын сүлжээнд ажиглагдсан цахим халдлагын үйл ажиллагааны гол үе шатуудыг ерөнхийд нь харуулж байна.



Нарийвчилсан цаг хугацааны дараалал

Долоодугаар сар: Халдагчид байгууллагад зориулан бүтээсэн веб аппликейшний (T1190) (цаашид “вэб програм” эсвэл “*webapp*” гэх) нүүр хуудсанд анхны холболтоо тогтоосон. Энэ үйлдэл нь Transport Layer Security (TLS) холболтоор хийгдсэн (T1102). Бусад анхаарал татахуйц үйл ажиллагаа энэ сард ажиглагдаагүй.

Долдугаар сар: Халдагч этгээдүүд байгууллагын веб аппликейшн рүү чиглэсэн сайтыг шалгаж, цааш судлах боломжтой сүлжээний төгсгөлийг (endpoints) тодорхойлох ажиллагааг эхлүүлэв [2].

Долдугаар сар: Халдагч этгээдүүд тодорхой нэг сүлжээний endpoint рүү чиглэсэн дайралтаа төвлөрүүлэв.

Долдугаар сар: Халдагч этгээдүүд веб сервер рүү амжилттай `POST` хүсэлт илгээж чадсан нь магадгүй өмнө нь өөр хуудас дээр байршуулсан арын хаалга (web shell) ашигласан байх боломжтой. Үүний дараа хоёр дахь IP хаяг мөн л ижил URL рүү хүсэлт илгээж эхэлсэн бөгөөд энэ нь магадгүй ижил халдагч бүлэгтэй холбоотой байх магадлалтай. Халдагч этгээдүүд хэд хэдэн магадлалтай арын хаалга (web shell) үүсгэж, туршсан байна.

Үнэн хэрэгтээ ашигласан арга нь тодорхойгүй боловч тодорхой нэг сүлжээний төгсгөл рүү чиглэсэн файл үүсгэх оролдлого явагдсан нь илэрхий бөгөөд энэ нь `<webapp>2-ext` хаяг дээр хийгдсэн.

ASD-ийн ACSC-ийн үзэж буйгаар дээрх хоёр IP-гийн холболт нь ижил халдлагын хүрээнд хийгдсэн байх өндөр магадлалтай бөгөөд хоорондын холболтууд нь хэдхэн минутын зайтай болсон нь үүнийг нотолж байна.

Долдугаар сар: Энэхүү бүлэглэл үйлдлээ үргэлжлүүлэн хостын мэдээллийг тодорхойлох (host enumeration) ажиллагаа хийж, нэвтрэх эрх нэмэгдүүлэх (privilege escalation) боломж хайж, өөр төрлийн арын хаалга (web shell) байршуулав. Тэд алдагдсан нууц үгээр `<firstname.surname>@<organisation domain>` хаягаар веб аппликейшн рүү нэвтэрчээ.

`<webapp>2-ext` дээр нэвтрэх эрх нэмэгдүүлэх үйлдэл амжилтгүй болсон бололтой. Үүний оронд, халдагч этгээдүүд сүлжээнд суурилсан үйл ажиллагаа руу шилжсэн.

Долдугаар сар: Халдагч этгээдүүд дотоодод нэвтрэх боломжтой хоёртын (binary) файлд хардкод хийгдсэн байх магадлалтай үйлчилгээний хаягт хэрэглэгчийн нэр, нууц үгийг ашиглаж шалгав.[3]

Долдугаар сар: Халдагч этгээдүүд open source хэрэгсэл болох Secure Socket Funnelling (SSF)-г байршуулсан бөгөөд уг хэрэгсэл нь мэдээллийг гадагш хортой дэд бүтэц рүү холбогдоход ашиглагдсан байна. Энэхүү холболтыг ашиглан халдагч талын төхөөрөмжүүдээс байгууллагын дотоод сүлжээнд туннел үүсгэн нэвтрэх оролдлого хийсэн бөгөөд бүртгэлд тухайн төхөөрөмжийн нэрс нь “service account” буюу үйлчилгээний аккаунт ашиглах оролдлогын үед ил болсон.

Наймдугаар сар: Халдагчид хязгаарлагдмал халдлагын ажиллагаа явуулсан бөгөөд үүнд “service account” буюу үйлчилгээний аккаунтыг ашиглан холболт тогтоох гэсэн амжилтгүй оролдлогууд орно.

Наймдугаар сар: Халдагч этгээдүүд сүлжээ болон “Active Directory” буюу удирдлагын системийг өргөн хүрээнд тодорхойлох ажиллагаа явуулсан. Үүний дараа өөр нэг алдагдсан эрхтэй хэрэглэгчийн бүртгэл ашиглан, DMZ-д байрлах [4]Windows төхөөрөмжүүд дээр network share-уудыг холболт хийснээр мэдээлэл гадагш зөөвөрлөгджээ.

Энэ нь DMZ бүсэд хандах боломжтой төхөөрөмжүүд дээр санамсаргүй байдлаар хулгайлагдсан нэвтрэх эрхийн мэдээллийг ашигласан байх магадлалтай. Хамгаалалтын систем (Firewalls) дотоод сүлжээг ижил аргаар онилох оролдлогыг хаасан байна.

Найм – Есдүгээр сар: SSF (Secure Socket Funnelling) хэрэгсэл дахин холбогдож, хортой IP хаяг руу сүлжээний туннел үүсгэсэн. Тухайн бүлэглэл өөр нэмэлт халдлага хийсэн нь нь тогтоогдоогүй бөгөөд тэдний хандалтыг хаах хүртэл идэвхгүй байжээ.

Есдүгээр сар: Байгууллага тухайн хортой IP-г хамгаалалтын систем (Firewalls) дээрээ denylist буюу хориглосон жагсаалтад оруулж блоклосон.

2 Энэ нөхцөлд “endpoint” гэдгийг нь веб аппликейшний функц гэсэн утгаар оруулсан болно.
3 “Service account” гэдэг нь тодорхой хэрэглэгч бус, харин үйлчилгээнд ашиглагддаг хэрэглэгчийн эрх юм. Microsoft домэйн орчинд янз бүрийн төрлийн хэрэглэгчийн бүртгэл байдаг.
4 “Mounting shares” гэдэг нь файл системийн бүтэц дэх файлуудыг хэрэглэгч болон хэрэглэгчийн бүлэгт хандах боломжтой болгох үйлдэл юм.

Халдагчийн ашигласан арга, техникүүд:

MITRE ATT&CK Framework нь цахим орчинд аюул занал учруулагч этгээдүүдийн хэрэглэдэг арга, техникүүдийг бүртгэн баримтжуулсан сан юм. Энэхүү санг АНУ-ын ашгийн төлөө бус байгууллага болох MITRE Corporation боловсруулсан бөгөөд дэлхий дахинд цахим заналхийллийн нийтлэг толь болгон ашигладаг.

ASD-ийн харьяа Цахим Аюулгүй Байдлын Төв (ASD's ACSC) дараах арга, техникүүдийн тухайн халдагч этгээдийн хортой үйл ажиллагаатай холбоотой гэж дүгнэж байна:

Халдлагын талаарх мэдээлэл цуглуулалт

T1594 – Хохирогчийн эзэмшлийн вебсайтыг шүүх

Халдагч тал байгууллагад зориулан бүтээсэн веб аппликейшний сайтын бүтцийг шалгаж, сүлжээнд нэвтрэх боломж хайсан.

Эхний нэвтрэлт

T1190 – Гадагш хандалттай аппликейшнүүдийг ашиглан нэвтрэх (Байгууллагын тусгай веб аппликейшнийг ашигласан үйлдэлтэй холбоотой)

T1078.002 – Хүчин төгөлдөр хэрэглэгчийн хаяг: Домэйн хэрэглэгчийн эрх (Хулгайлагдсан хэрэглэгчийн эрхийг ашиглан системд нэвтэрсэнтэй холбоотой)

Интернэтэд нээлттэй байршуулсан тусгай веб аппликейшнийг ашигласнаар халдагч этгээд сүлжээнд анхны хандалт үүсгэж чадсан. Үүний дараа тэд өмнө нь хулгайлсан нэвтрэх мэдээллүүдийг ашиглан сүлжээнд илүү өргөн хүрээгээр хандах боломжтой болсон.

Гүйцэтгэл

T1059 – Command and Scripting Interpreter программ (Арын хаалга (web shell)-ээр дамжуулан удирдахтай холбоотой)

T1072 – Програм хангамж түгээх хэрэгслүүд (Халдагч этгээд Secure Socket Funnelling (SSF) гэх үнэгүй хэрэгслийг ашиглан IP хаяг руу холбогдсон үйлдэлтэй холбоотой)

Тогтвортой нэвтрэлт (Persistence)

T1505.003 – Серверийн програм хангамжийн бүрдэл хэсэг: Арын хаалга (Web Shell) (Халдагч этгээд арын хаалга болон SSF ашиглан сүлжээнд дахин нэвтрэх тогтвортой хандалт тогтоосон үйлдэлтэй холбоотой)

Нэвтрэх мэдээлэл хулгайлах

T1552.001 – Нууц үг хадгалах сангаас мэдээлэл хулгайлах (Барилгын удирдлагын систем (BMS)-тэй холбоотой нууц үг хадгалагдсан файлуудтай холбоотой)

T1558.003 – Керберос код хулгайлах эсвэл хуурамчаар үйлдэх: Керберос ашиглан халдах (Сүлжээний нэвтрэх эрх олж авах зорилгоор Керберос халдлагыг хийсэнтэй холбоотой)

Хөндлөн шилжилт

T1021.002 – Зайнаас хандах үйлчилгээ: SMB хуваалтууд (Халдагч этгээд олон төхөөрөмжөөс SMB хуваалтуудыг холбосон үйлдэлтэй холбоотой)

Цуглуулалт

T1213 – Мэдээллийн агуулахуудаас мэдээлэл авах (BMS сервер дээрх гарын авлага, техникийн баримт бичгүүдтэй холбоотой)

Мэдээлэл хууль бусаар зөөвөрлөх

T1041 – Команд ба хяналтын сувгаар мэдээлэл алдагдуулах (Exfiltration Over C2 Channel) (Active Directory болон холбосон сүлжээний хуваалтуудаас өгөгдөл алдагдсан үйл ажиллагаатай холбоотой)

Жишиг судалгаа 2

Энэхүү тайланг олон нийтэд өргөн хүрээнд түгээх зорилгоор нэрийг нууцалсан болно. Халдлагад өртсөн байгууллагыг цаашид "байгууллага" гэж нэрлэнэ. Хохирогч байгууллагын үнэн зөв байдлыг хадгалах болон ASD-ийн ACSC-гийн хариу арга хэмжээний аргачлалыг хамгаалах үүднээс тодорхой мэдээллийг хассан болно.

Товч хураангуй

Энэхүү тайлан нь 2022 оны 4-р сард байгууллагын сүлжээнд амжилттай нэвтэрсэн халдлагын талаар ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC)-ийн явуулсан мөрдөн шалгалтын үр дүнг нэгтгэсэн болно. Мөрдөн шалгалтын энэхүү тайланг тухайн байгууллагад хүргүүлсэн бөгөөд илэрсэн халдлагын үйл ажиллагааг нэгтгэн дүгнэж, хамгаалалт, сэргээлтийн зөвлөмжийг хүргэсэн болно. Мөрдөн шалгалтын үр дүнд энэхүү халдлагыг APT40 бүлэглэл үйлдсэн болохыг тогтоосон.

2022 оны тавдугаар сард ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC) нэгэн байгууллагад хандан тэдний сүлжээнд 2022 оны дөрөвдүгээр сараас хойш халдлагууд ажиглагдсан талаар анхааруулсан. Үүний дараагаар тус байгууллага нь интернэтэд холбогдсон нэгэн сервер дээрээ сэжиг бүхий хортой программ илрүүлсэн тухай ACSC-д мэдэгдсэн бөгөөд уг сервер нь байгууллагын албан хэрэгцээний зайнаас хандалтын системийн нэвтрэх порталаар ашиглагдаж байсан. Энэ сервер нь зайнаас нэвтрэх эрх болон хэрэглэгчийн таних мэдээлэл удирдах зориулалттай бүтээгдэхүүн агуулж байсан бөгөөд энэхүү тайланд “зөвшөөрөлгүй нэвтэрсэн төхөөрөмж” (the compromised appliance) хэмээн нэрлэгдэх болно. Энэхүү тайланд ASD-ийн ACSC-аас явуулсан мөрдөн шалгалтын үр дүн, мөн тухайн байгууллагад зориулан боловсруулсан сэргээх арга хэмжээний зөвлөмжүүдийг тусгасан болно.

Шалгалтаар тухайн байгууллагын сүлжээний нэг хэсэг нь 2022 оны дөрөвдүгээр сараас хойш зайнаас хандах портал-аар дамжуулан цахим халдагчдын гарт орсон болох нь тогтоогдсон. Мөн уг сервер нь тухайн үеийн олон нийтэд ил болсон Remote Code Execution (RCE) төрлийн сул талыг ашигласан байх магадлалтай бөгөөд ганц биш, хэд хэдэн халдагчийн зүгээс нэвтрэлт хийсэн байх боломжтой.

ASD-ийн ACSC-гийн баг дараах гол үйл ажиллагааг илрүүлсэн:

- Хост тандах (Host Enumeration) – Халдагч тал байгууллагын сүлжээний бүтцийн зураглал үүсгэдэг..
- Интернэтэд нээлттэй програм, веб апликэйшнийг ашиглан нэвтрэх болон арын хаалга (websshell) ашиглах. Энэ нь халдагч талд сүлжээнд анхлан нэвтрэх, удирдлагыг алсаас илгээх боломжийг олгодог.
- Програм хангамжийн сул талыг ашиглан нэвтрэх эрх нэмэгдүүлэх,
- мөн сүлжээнд дотоод шилжилт хийхэд шаардлагатай нэвтрэх бүртгэлийн мэдээлэл цуглуулах зэрэг үйлдлүүд хийгдсэн байв.

ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC)-ийн шалгалтаар 2022 оны дөрөвдүгээр сард зөвшөөрөлгүй хандсан төхөөрөмж дээрээс хэдэн зуун өвөрмөц хэрэглэгчдийн нэр, нууц үг зөөвөрлөгдсөн нь тогтоогдсон. Түүнчлэн зайнаас хандахад шаардлагатай давхар баталгаажуулалтын код алдагдсан байж болох ул мөрүүд олдсон байна. Байгууллагын дотоод хяналт, шалгалтаар эдгээр нууц үгс нь хүчинтэй, бодит хэрэглэгчидтэй холбоотой болох нь батлагдсан. ASD-ийн ACSC-ийн дүгнэж буйгаар, уг халдагч эдгээр цахим мэдээллийг ашиглан жинхэнэ хэрэглэгчийн нэрийн өмнөөс зайнаас нэвтрэлт хийх, улмаар байгууллагын дотоод сүлжээнд хууль бус байдлаар хандах зорилготой байсан байх өндөр магадлалтай.

Мөрдөн шалгалтын дүн

Мөрдөн шалгалтын тойм

ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC)-ийн үнэлгээгээр цахим халдагч нь байгууллагын ажилтнуудын зайнаас нэвтрэх төхөөрөмжүүд рүү халдаж, улмаар түүгээр дамжуулан нэмэлт сэжигтэй үйл ажиллагаа явуулахыг оролдсон байна. Эдгээр төхөөрөмж нь хоорондоо ачаалал тэнцвэржүүлэгчтэй гурван хостуудаас бүрддэг бөгөөд хамгийн эхний халдлагын ул мөр гурван хост дээр илэрсэн. Халдлагын анхны шинж тэмдгүүд илэрсний дараахан байгууллага хоёр хостыг унтраасан. Үүний улмаас дараагийн бүх сэжигтэй үйлдлүүд үлдсэн ганц хост дээр явагдсан байна. Халдлагад өртсөн төхөөрөмжтэй холбоотой бусад серверүүд ч мөн ачаалал тэнцвэржүүлэгчтэй бүтэцтэй байсан. Илүү ойлгомжтой болгохын тулд, тайлангийн ихэнх хэсэгт эдгээр төхөөрөмжүүдийг "нэг төхөөрөмж" гэж нэрлэсэн болно.

Халдагч этгээдүүд нь 2022 оны дөрөвдүгээр сараас эхлэн олон нийтэд ил болсон сул байдлыг ашиглан уг төхөөрөмж дээр арын хаалга (webshell) байршуулсан гэж үзэж байна. Мөн халдагч нь уг төхөөрөмж дээр нэвтрэх эрх нэмэгдүүлэлт хийж, хяналт тогтоосон гэж дүгнэгджээ. ASD-ийн ACSC нь лог бүртгэл хязгаарлагдмал байсан тул халдлагын цар хүрээг бүрэн тодорхойлж чадаагүй. Гэсэн хэдий ч төхөөрөмж дээрх нотолгооноос харахад дараах үйлдлүүд хийгдсэн нь тогтоогдсон:

- Хэдэн зуун бодит хэрэглэгчийн нэр, нууц үгийн хослосон мэдээллийг цуглуулсан;
- Мөн тус төхөөрөмжөөс хортой этгээдүүд виртуал десктоп дэд бүтцийн (VDI) хандалтад жинхэнэ хэрэглэгчийн нэрээр нэвтрэх боломж олгох цахим мэдээлэл цуглуулсан нь тогтоогдсон.

ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC)-ийн үнэлгээгээр, халдагч этгээдүүд байгууллагын сүлжээнд цааш халдах, илүү гүнзгий хяналт тогтоох зорилготой байсан байх магадлалтай. Халдагчийн гадагш зөөвөрлөсөн эдгээр мэдээлэлэ нь тухайн этгээдийг өөрийн сонгосон жинхэнэ хэрэглэгчийн эрхээр буюу удирдлагын эрхтэй хэрэглэгчийн нэрээр VDI хандалт рүү хууль бусаар нэвтрэх, эсвэл хандалт эхлүүлэх боломжийг олгосон байж болзошгүй. Энэ төрлийн нэвтрэлтийг ашиглан халдагч этгээд байгууллагын дотоод үйлчилгээ, системийг илүү өргөн хүрээтэй хянах, тогтвортой нэвтрэх эрх (persistence) бий болгох, бусад зорилгоор ашигласан байх магадлалтай.

Тухайн төхөөрөмжийн хостинг үйлчилгээ үзүүлэгч бусад ижил төстэй төхөөрөмжүүд дээр халдлагын ул мөр илрээгүй болно.

Хандалт

Халдлагад өртсөн төхөөрөмжийн хост нь хэрэглэгч VDI (Виртуал Десктоп Дэд бүтэц) хандалтрүү холбогдох үед Active Directory болон вэб серверээр дамжуулан баталгаажуулалт хийдэг байсан (T1021.001).

Байршил	Халдлагад өртсөн төхөөрөмжүүдийн хост нэрс (ачаалал тэнцвэржүүлсэн):
Дата төв 1	HOST1, HOST2, HOST3

Халдлагад өртсөн төхөөрөмжийн дэд бүтэц нь хэрэглэгч баталгаажуулалтын токен хүлээн авсны дараа Виртуал Десктоп Дэд бүтэц (VDI)-д холбогдох туннел (суваг) үүсгэдэг хандалтын гарц хостууд (access gateway hosts)-ыг мөн агуулж байсан.

Эдгээр хандалтын гарц хостууд халдлагад өртсөн гэсэн шууд нотолгоо олдоогүй. Гэсэн хэдий ч, эдгээр хостуудын мэдээллийн бүртгэлд сэжигтэй, хортой үйл ажиллагаанд холбогдож байсан IP хаягуудтай их хэмжээний холбоо тогтоосон байсныг харуулсан ул мөр илэрсэн. Энэ нь уг хост дээр шууд үйлдэл хийгдсэн эсвэл тухайн хост руу гадны заналхийлэгчийн дэд бүтэцтэй холбогдсон сүлжээний харилцаа үүссэн байх боломжтойг илтгэнэ. Одоогоор байгаа нотолгоонд тулгуурлан үйл ажиллагааны нарийн шинж чанарыг бүрэн тогтоох боломжгүй байгаа боловч, уг бүлэглэл нь байгууллагын сүлжээгээр шилжих (lateral movement) оролдлого хийж байсныг харуулж байна (TA0008).

Дотоод хостууд

ASD-ийн Цахим Аюулгүй Байдлын Төв (ACSC) нь тус байгууллагын дотоод сүлжээний сегментээс бага хэмжээний мэдээлэл авч, шинжилгээ хийсэн. Байгууллагын дотоод сүлжээний сегментэд нөлөөлсөн буюу нөлөөлөхийг оролдсон халдлагын мэдэгдэж буй үйлдлүүдэд дараах зүйлс багтана. Үүнд: VDI-тэй холбоотой баталгаажуулалтын өгөгдөлд хандах; байгууллагын дотоод SQL серверээс мэдээлэл хуулж авах үйлдэл (T1505.001); мөн мэдэгдэж буй хортой IP хаягуудаас гарсан сэжигтэй сүлжээний урсгал нь хандалтын гарц төхөөрөмж (access gateway appliance)–аар дамжин өнгөрсөн байна (TA0011).

Цахим гэмт этгээдүүд төхөөрөмжид хандах боломжоор дамжуулан жинхэнэ хэрэглэгчийн нэр, нууц үг (T1003), олон үе шаттай баталгаажуулалтын (MFA) код (T1111) цуглуулсан байна. Мөн виртуал десктоп хандалт үүсгэхэд хэрэглэгддэг JSON Web Token (JWT) зэрэг баталгаажуулалтын мэдээлэл цуглуулсан байна (T1528). Цуглуулсан эдгээр мэдээллийг ашиглан виртуал десктоп орчныг хууль ёсны хэрэглэгчийн нэрээр үүсгэх

эсвэл булаан авах (T1563.002) замаар байгууллагын дотоод сүлжээнд хууль ёсны эрхтэй мэт хандах (T1078) боломжтой болсон байж болзошгүй.

Мөн уг төхөөрөмжөөр дамжуулан байгууллагын дотоод сүлжээнд байрлах SQL серверээс мэдээлэл татах буюу "scrape" хийх ажиллагаа гүйцэтгэсэн нь тогтоогдсон (T1505.001). Энэхүү өгөгдөлд халдагч этгээд нэвтрэх эрхтэй байсан байх магадлалтай.

Нэвтрэх гарцын төхөөрөмжөөс олдсон нотолгоо нь хортой IP хаягууд энэ төхөөрөмжөөр дамжин сүлжээний урсгал явагдсан болохыг харуулж байна. Дээр дурдсанчлан, энэ нь цахим гэмт этгээдүүд тус төхөөрөмжид нөлөөлсөн буюу халдсан байж магадгүй бөгөөд үүний тусламжтайгаар дотоод сүлжээнд нэвтрэхийг оролдсон байж магадгүйг харуулж байна.

Шалгалтын үйл явцын цаг хугацааны дараалал

Доорх жагсаалт нь шалгалтын явцад илрүүлсэн гол үйл ажиллагааны цаг хугацааны дарааллыг харуулна.

Цаг	Үйл явдал
2022 оны 4-р сар	Халдлага үйлдэгчтэй холбогдсон нэр бүхий хортой IP хаягууд HOST7 сервертэй харилцсан. Эдгээр холболтын нарийн шинж чанарыг тодорхойлох боломжгүй байв.
2022 оны 4-р сар	HOST1, HOST2 болон HOST3 бүх серверүүд халдлагад өртсөн бөгөөд дээрх серверүүд дээр арын хаалга (webshell) байрлуулсан. HOST2 дээр бүртгэлийн лог файлууд үүсгэгдсэн эсвэл засварлагдсан. Тухайн файлд хэрэглэгчийн нэр, нууц үгийн мэдээлэл агуулагдаж байх магадлалтай. HOST1 болон HOST3 серверүүд дээрх “/etc/security/opasswd” болон “/etc/shadow” системийн файлууд өөрчлөгдсөн нь нууц үг солигдсоныг илтгэж байна Мөн HOST1 дээрх нотолгооноос үзэхэд “sshuser” хэрэглэгчийн нууц үг өөрчлөгдсөн байна.
2022 оны 4-р сар	HOST2-ыг байгууллага унтраасан. HOST1 болон HOST3 дээр нэмэлт арын хаалгууд (webshell) (T1505.003) үүссэн. HOST3-аас HOST1 руу SSH нэвтрэх эрхийн халдлагын оролдлогууд илэрсэн. HOST3 дээр бүртгэлийн лог файл засварлагдсан (T1070). Энэхүү файлд магадгүй халдагч этгээдийн авсан хэрэглэгчийн нэр, нууц үгийн мэдээлэл (T1078) агуулагдаж байна. JWT-ууд цуглуулж, HOST3 дээр хадгалагдсан байна (T1528). HOST3-ыг байгууллага унтраасан. Үүний дараах бүх үйл ажиллагаа HOST1 дээр явагдсан.
2022 оны 4-р сар	HOST1 дээр нэмэлт арын хаалгууд (webshell) үүссэн (T1505.003). JWT-үүдийг цуглуулж, HOST1 дээр файл гаргасан.
2022 оны 4-р сар	HOST1 дээр нэмэлт арын хаалгууд (webshell) үүссэн (T1505.003) ба хортой IP хаяг уг сервертэй холбогдсон (TA0011). Хортой IP хаяг ACCESS GATEWAY-ийн HOST7 сервертэй холбогдсон.
2022 оны 5-р сар	Хортой IP хаяг ACCESS GATEWAY-ийн HOST7 сервертэй холбогдсон (TA0011). HOST1 дээрх бүртгэлд хэрэглэгчийн нэвтрэлт нь хортой IP хаягтай холбогдсон. Энэхүү сервер дээр нэмэлт арын хаалга (webshell) үүссэн (T1505.003).
2022 оны 5-р сар	Халдагч этгээдийн үйлдлээр HOST1 дээрх скрипт өөрчлөгдсөн (T1543). Энэхүү скрипт нь дотоод SQL серверээс өгөгдөл авдаг функцтэй байжээ.
2022 оны 5-р сар	HOST1 дээр нэмэлт бүртгэлийн лог файл сүүлд засварлагдсан (T1070). Энэхүү файлд байгууллагын сүлжээнд ашиглагдсан хэрэглэгчийн нэр, нууц үг байгаа бөгөөд тэдгээр нь жинхэнэ хаягуудын нэвтрэх эрхийн мэдээлэл гэж үзэж байна (T1078).
2022 оны 5-р сар	Нэмэлт бүртгэлийн лог файл сүүлд засварлагдсан (T1070). Энэ файлд HOST1-ээс цуглуулсан JWT-үүд агуулагдаж байна.
2022 оны 5-р сар	HOST1 дээр нэмэлт арын хаалгууд (webshell) үүссэн (T1505.003). Энэ өдөр байгууллага 2022 оны 4-р сард үүсгэсэн арын хаалга (webshell) олдсоныг ASD-ийн ACSC-д мэдээлсэн.
2022 оны 5-р сар	HOST1 дээр хэд хэдэн скрипт үүссэн, түүний дотор Log4jHotPatch.jar нэртэй файл орсон.
2022 оны 5-р сар	iptables-save командыг ашиглан ACCESS GATEWAY-ийн серверт 2 нээлттэй порт нэмсэн. Эдгээр портууд нь 9998 ба 9999 байв (T1572).

Цахим халдагчийн тактик, техникийг онцолсон хэсэг

Шалгалтын явцад илэрсэн хэд хэдэн арга техникүүдийг доор дурдсан байна.

Эхний нэвтрэлт

T1190 Интернэтэд холбогдсон аппликейшний сул талыг ашиглах

Халдлагын бүлэг нь зайнаас хандалт болон таних удирдлагын системүүдийн алсын код гүйцэтгэх (RCE), нэвтрэх эрх нэмэгдүүлэх, баталгаажуулалтыг алгасах, тойрох зэрэг эмзэг байдлыг ашиглан байгууллагын сүлжээнд анхны нэвтрэлтийг хийсэн байх өндөр магадлалтай гэж үзэж байна.

Энэхүү анхны нэвтрэх аргыг хамгийн магадлалтай гэж үзэж байгаа нь дараахтай холбоотой:

- Халдлага үйлдэгдсэн тухайн үед сервер нь нийтэд танигдсан CVE-үүдэд өртөмтгий байсан;
- Нэр бүхий халдагч этгээдийн хяналттай дэд бүтцээс эдгээр сул талыг ашиглах оролдлогууд хийсэн нь бүртгэгдсэн;
- Эдгээр оролдлогын дараахан дотоод сүлжээнд анхны халдлагын үйлдлүүд илэрсэн.

Гүйцэтгэл

T1059.004 Command and Scripting Interpreter програм: Юникс арын хаалга (Unix webshell)

Халдлагын бүлэг дээр дурдсан сул талуудыг амжилттай ашигласнаар, халдварласан төхөөрөмж дээрх Юникс арын хаалгаар дамжуулан командыг гүйцэтгэх боломжтой болсон байх магадлалтай. Төхөөрөмж дээрх бүртгэлийн бүрэн бус байдал нь халдагч этгээдүүдийн гүйцэтгэсэн командуудыг бүрэн тодорхойлоход хүндрэл учруулж байна.

Тогтвортой нэвтрэх

T1505.003 Серверийн Программ Хангамжийн Бүрэлдэхүүн Хэсэг: Арын хаалга (webshell)

Халдагч этгээдүүд нэвтэрсэн төхөөрөмжид хэд хэдэн арын хаалга (webshell) байршуулсан. Мөн энэ хугацаанд өөр өөр бүлэглэлүүд арын хаалгуудыг (webshell) байршуулсан байх магадлалтай боловч зөвхөн цөөн тооны бүлэглэл эдгээрийг идэвхтэй ашигласан байх үндэслэлтэй байна. Арын хаалгууд (webshell) нь халдагч этгээдэд төхөөрөмж дээр дурын командыг гүйцэтгэх боломжийг олгосон.

Нэвтрэх эрхийн нэмэгдүүлэлт

T1068 Нэвтрэх эрх нэмэгдүүлэх зорилгоор сул талуудыг ашиглах

Халдагч этгээдүүдийн ямар түвшний удирдлагын эрхтэй байсныг бүрэн тодорхойлох боломжгүй Гэсэн хэдий ч арын хаалга ашигласнаар тэдгээр нь веб серверийн хэрэглэгчийн эрхтэй дүйцэхүйц түвшинд команд гүйцэтгэх боломжтой болсон гэж дүгнэж байна. Халдлагад өртсөн төхөөрөмжийн сул талуудыг ашиглан халдагч этгээдүүд гол нэвтрэх эрхийг олж авсан байх боломжтой гэж үзэж байна.

Нэвтрэх мэдээлэл хулгайлах

T1056.003 Оруулах өгөгдөл хулгайлах: Веб портал эзлэх

Халдсан төхөөрөмжөөс олдсон нотолгооноос харахад, халдагч этгээд хэдэн зуун тооны хэрэглэгчийн нэр болон нууц үгийн хослолыг текст бичгэн хэлбэрээр гарган авсан байна. Эдгээр мэдээллүүд нь жинхэнэ хэрэглэгчдийнх байх магадлалтай. Эдгээр мэдээллүүдийг бодит баталгаажуулалтын процессыг өөрчилж, нэвтрэх эрхийн мэдээллийг файл руу хадгалах замаар хураан авсан гэж үзэж байна.

T1111 Давхар баталгаажуулалтын мэдээллийг олзлох

Халдагч этгээд мөн олон шатлалт баталгаажуулалтын (MFA) токенуудыг олзолсон авсан бөгөөд эдгээр нь жирийн хэрэглэгчийн жинхэнэ нэвтрэлттэй холбоотой байсан. Эдгээр мэдээлэл нь, хэрэглэгчийн нэвтрэлтийн процессыг өөрчлөх замаар, токен утгуудыг файлд бичиж хадгалах хэлбэрээр олзолсон байх магадлалтай. Гэсэн хэдий ч MFA токены хамгаалалт хариуцсан ‘нууц сервер’ нь халдлагад өртсөн нотолгоо байхгүй байна.

T1040 Сүлжээний мэдээлэл тагнах

JSON Web Token (JWT)-уудыг хураахдаа халдагч этгээд HTTP протоколын сүлжээний урсгалыг тагнасан гэж үзэж байна. Халдсан төхөөрөмж дээр tcpdump хэрэгслийг ажиллуулсан нотолгоо байгаа бөгөөд энэ нь этгээд JWT-үүдийг ингэж олзолсон байж магадгүй.

T1539 Веб хандалтын күүки хулгайлах

Дээр дурдсанчлан, этгээд JWT-үүдийг хураасан бөгөөд эдгээр нь веб хандалтын күүкитэй адил юм. Эдгээрийг халдагч этгээд дахин ашиглан сүлжээнд нэмэлт нэвтрэлт хийх боломжтой байжээ.

Илрүүлэлт

T1046 Сүлжээний үйлчилгээний илрүүлэлт

Нотлох баримтуудаас харахад халдагч этгээд нь нэвтэрсэн төхөөрөмж дээр “nmap” хэмээх сүлжээний сканнер хэрэгслийг ажиллуулж, тухайн дотоод сүлжээний сегментэд байгаа бусад төхөөрөмжүүдийг шалгасан байна. Энэ нь тухайн сүлжээнд холбогдож болохуйц үйлчилгээ, хостуудыг илрүүлэх зорилготой байсан бөгөөд улмаар цааш дамжин халдах (lateral movement) боломжуудыг тодорхойлохыг зорьсон бололтой.

Цуглуулга

Халдлагад өртсөн төхөөрөмж болон холбогдох бусад системүүдээс халдагч этгээд хэрхэн мэдээлэл цуглуулсан, яг ямар өгөгдөл авсан нь одоогоор бүрэн тодорхойгүй байна. Гэсэн хэдий ч халдлагад өртсөн төхөөрөмж дээр хураагдсан нэвтрэх нэр, нууц үгийн хослолууд (T1003), давхар баталгаажуулалтын токенууд (T1111) болон дээр дурдсан JWT-үүдийг хамран бүх файлуудад нэвтрэх эрхтэй байсан гэж үзэж байна.

Команд ба хяналт

T1071.001 Программын давхаргын протокол: Веб протоколууд

Халдагч этгээдүүд команд удирдлага үүрэгтээ арын хаалгуудыг (webshell) ашигласан. Арын хаалгын (webshell) командууд төхөөрөмж дээр байгаа веб серверээр дамжуулан HTTPS протоколоор дамжиж илгээгдсэн байна (T1572).

T1001.003 Өгөгдөл нуух: Протоколыг дууриах

Халдагч этгээдүүд халдлагад өртсөн төхөөрөмжүүдийг хууль ёсны сүлжээний урсгал дунд нуугдах зорилготой халдлагын эхлэл цэг болгон ашигласан байна .

Халдлагын аюулыг илрүүлэх болон сэргийлэх зөвлөмжүүд

ASD-ийн ACSC нь ASD Нэн шаардлагатай найман хяналтын арга хэмжээ хяналтууд болон холбогдох Цахим аюулгүй байдлын халдлагыг хязгаарлах стратегиудыг хэрэгжүүлэхийг хатуу зөвлөж байна. Доорх хэсэгт APT40 бүлгийн халдлагыг илрүүлэх, урьдчилан сэргийлэхэд чиглэсэн сүлжээний хамгаалалтын үндсэн арга хэмжээнүүд болон Хүснэгт 1-д дурдсан голлох дөрвөн тактик, техник, ажиллагааны (TTP) хязгаарлалтын нарийвчилсан зөвлөмжүүдийг багтаав.

Илрүүлэлт

Дээр дурдсан зарим файлуудыг C:\Users\Public* болон C:\Windows\Temp* зэрэг байршлуудад байршуулсан байна. Эдгээр байршлууд нь ихэвчлэн дэлхий нийтээр бичих эрхтэй буюу Windows-д бүртгэлтэй бүх хэрэглэгчдэд хандах эрхтэй байдаг тул өгөгдөл бичихэд тохиромжтой байдаг. Ихэнх тохиолдолд ямар ч хэрэглэгч эдгээр байршилд хадгалагдсан файлуудад хандах боломжтой байдаг. Үүний улмаас халдагчид дараах үйлдлүүдийг хийх боломжтой болно: сүлжээнд дамжин нэвтрэх, хамгаалалтаас зайлсхийх, хязгаарлагдмал эрхтэйгээр команд гүйцэтгэх, мэдээлэл хулгайлах бэлтгэл хийх зэрэг.

Доорхи Sigma дүрмүүд сэжигтэй байршлуудаас гүйцэтгэл явагдаж байгаа эсэхийг хянан, хэвийн бус үйлдлийн шинж тэмдгийг илрүүлнэ. Бүх тохиолдолд гэмт үйлдэл, халдагч этгээдийн шинжийг бататгахын тулд нэмэлт мөрдлөг шаардлагатай болно.

Гарчиг: Дэлхийн бичих эрхтэй байршлаас гүйцэтгэл илрүүлэх - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Тайлбар C:\Windows\Temp*-аас процессын гүйцэтгэл илрүүлэх.

Үндсэн мэдээлэл

Энэхүү дүрэм нь C:\Windows\Temp*-аас гүйцэтгэгдэж байгаа үйлдлийг онцгойлон хянахад зориулагдсан. Temp хавтас нь програмуудын хэвийн ажиллагаанд түгээмэл хэрэглэгддэг тул энэ хавтаснаас үүссэн гүйцэтгэлийг сэжигтэй гэж үзэх магадлал бусад бүх C:\Windows дэх нийтийн бичих эрхтэй хавтаснуудаас бага байдаг.

SYSTEM эсвэл NETWORK SERVICE хэрэглэгчийн нэрээр ажиллаж байгаа програмуудыг хасах нь энэ дүрмээр сонгогдож буй энгийн үйлдлийн тоог мэдэгдэхүйц бууруулна.

Энэ дүрэм нь өндөр эрхийн түвшинд гүйцэтгэгдэж буй аюултай үйлдлийг илрүүлж чадахгүй байж магадгүй ч, хэрэглэгч SYSTEM эрх авах оролдлого хийж байгаа эсэхийг шалгахын тулд бусад дүрмийг ашиглахыг зөвлөж байна.

Мөрдлөг:

1. Энэ файл гүйцэтгэсэнтэй холбоотой хэрэглэгчийн агуулга, гүйцэтгэлийн эрхийн түвшин, дараалсан үйлдлүүд болон файл ачаалсан дүрсүүдийг шууд судална уу.
2. Хост дээрх процесс, сүлжээ, файл болон бусад дэмжих өгөгдлийг судалж, үйл ажиллагаа аюултай эсэхийг үнэлэхэд тусална.
3. Хэрэв шаардлагатай бол тухайн файлын хуулбарыг авч буцаах инженерчлэл хийх замаар хууль ёсны эсэхийг тодорхойлохыг оролдоно.

Эх сурвалжууд:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Зохиогч: ASD-ийн ACSC

Огноо: 2024/06/19

Төлөв: туршилтын шатанд

Тагууд:

- tlp.green
- classification.au.official
- attack.execution

Бүртгэлийн эх сурвалж:

ангилал: процесс үүсгэлт
бүтээгдэхүүн: windows

Илрүүлэлт:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}\}\\'
системийн_хэрэглэгч:
    Хэрэглэгч:
    - ‘СИСТЕМ’
    - ‘СҮЛЖЭЭНИЙ ҮЙЛЧИЛГЭЭ’
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path эсвэл system_user эсвэл dismhost эсвэл known_parent)

Хуурамч эерэг тохиолдлууд:

- Allowlist-аар баталгаажсан аудитын програмууд Temp хавтаснаас гүйцэтгэгдэх файлуудыг ажиллуулж байгаа нь ажиглагдсан.
- Temp нь олон төрлийн суулгагч болон эхлүүлэгч програмуудыг хууль ёсоор агуулдаг тул энэ дүрмийг хэрэгжүүлэхээс өмнө сүлжээнд хэр түгээмэл байгааг (болон зөвшөөрөх жагсаалтад оруулах эсэхийг) авч үзэх хэрэгтэй.

Түвшин: бага

Гарчиг: World Writable Execution - Non-Temp System Subdirectory

ID 5b187157-e892-4fc9-84fc-aa48aff9f997

Тайлбар: Windows үйлдлийн систем суусан байршил дэх бичих эрхтэй дэд хавтаснаас процессийн гүйцэтгэлийг илрүүлэх.

Үндсэн мэдээлэл:

Энэхүү дүрэм нь C:\ хавтас доторх дэлхий нийтийн бичих эрхтэй хавтаснаас, ялангуяа C:\Windows* хавтаснаас гүйцэтгэгдэж буй үйлдлийг онцгойлон хянахад зориулагдсан бөгөөд C:\Windows\Temp хавтсыг оруулаагүй (энэ нь энгийн програмуудаар өргөн ашиглагддаг тул аюултай үйлдэл гэх баталгаа багатай).

AppData хавтас нь файлыг SYSTEM эрхээр ажиллуулсан тохиолдолд хасагддаг бөгөөд энэ нь ихэнх тохиолдолд түр хугацааны програмын файлуудыг аюулгүйгээр ажиллуулах арга юм.

Анхны сүлжээний үндсийг тогтоож, эдгээр байрлалаас гарах аюулгүй гүйцэтгэлийг тодорхойлсны дараа энэ дүрэм цөөн тохиолдолд идэвхжих ёстой.

Мөрдлөг:

1. Тухайн файлын гүйцэтгэлтэй шууд холбогдох мэдээллийг шалгах, тухайлбал хэрэглэгчийн контекст, гүйцэтгэлийн эрхийн түвшин, дараалсан шууд үйлдэл болон файлын ачаалсан дүрсүүдийг судлах.
2. Аюултай үйлдэл эсэхийг үнэлэхэд туслах зорилгоор тухайн систем дээрх процесс, сүлжээ, файл болон бусад дэмжих мэдээллийг шинжлэх.
3. Хэрэв шаардлагатай бол уг файлын хуулбарыг авч, буцаах инженерчлэлийн замаар файлын хууль ёсны эсэхийг тогтоохыг оролдох.

Эх сурвалжууд:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Зохиогч: ASD-ийн ACSC

Огноо: 2024/06/19
Төлөв: туршилтын шатанд

Тагууд:

- tlp.green
- classification.au.official
- attack.execution

Лог бүртгэлийн эх сурвалж:

ангилал: process_creation
бүтээгдэхүүн: windows

Илрүүлэлт:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'

- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Зураг|агуулга: '\\AppData\\'
Хэрэглэгч: 'СИСТЕМ'

нөхцөл: writable_path ба appdata биш байх

Хуурамч эерэг тохиолдлууд:

Эдгээр хавтаснаас гүйцэтгэгдэх файлуудыг Allowlist хяналтын програмууд ажиллуулж байгаа нь ажиглагдсан.

Хяналт дор байгаа орчинд хэрэглэгддэг скрипт болон удирдлагын хэрэгслүүд эдгээр хавтаснуудад байрлаж байх магадлалтай тул тохиолдол тус бүрт тусгайлан авч үзэх шаардлагатай.

Түвшин: өндөр

Гарчиг: Дэлхий нийтийн бичих эрхтэй гүйцэтгэл – Хэрэглэгчид

ID: 6dda3843-182a-4214-9263-925a80b4c634

Тайлбар: C:\Users\Public* болон Users хавтас доторх дэлхий нийтийн бичих эрхтэй бусад хавтаснаас процесс гүйцэтгэгдэж буйг илрүүлэх.

Үндсэн мэдээлэл:

Хэрэв файл SYSTEM эрхээр ажиллаж байгаа бол AppData хавтаснуудыг энэ илрүүлэгт оруулдаггүй — учир нь олон төрлийн түр зуурын программын файлууд ийм байдлаар аюулгүй гүйцэтгэгддэг.

Мөрдлөг:

1. Энэ файлын гүйцэтгэлтэй шууд холбоотой мэдээллийг нарийвчлан шалгаарай, тухайлбал хэрэглэгчийн орчин, гүйцэтгэлийн бүрэн бүтэн байдлын түвшин, дараах шууд үйлдэл болон файл ачаалсан дүрслэлүүдийг гэх мэт.
2. Хост дээрх процесс, сүлжээ, файл болон бусад холбогдох мэдээллийг судалж, уг үйлдэл нь халдлага үйлдэх зорилготой эсэхийг шалгахад тусламж аваарай.
3. Хэрэв шаардлагатай бол тухайн файлын хуулбарыг цуглуулж, түүнийг хуулбарлах, буцаах инженерчлэл хийх замаар хууль ёсны эсэхийг тодорхойлоорой.

Эх сурвалжууд:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Зохиогч: ASD-ийн ACSC

Огноо: 2024/06/19

Төлөв: туршилтын шатанд

Тагууд:

- tlp.green
- classification.au.official
- attack.execution

Лог Бүртгэлийн эх сурвалж:

ангилал: process_creation
бүтээгдэхүүн: windows

Илрүүлэлт:

Хэрэглэгч:

Зураг|агуулга:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Зураг|агуулга: '\\AppData\\'
Хэрэглэгч: 'СИСТЕМ'

нөхцөл: writable_path ба appdata биш байх

Хуурамч эерэг тохиолдлууд:

- Хяналтанд байгаа орчинд ашиглагддаг скрипт болон удирдлагын хэрэгслүүд Public хавтас болон түүний дэд хавтаснуудад байрлах магадлалтай тул тохиолдол тус бүрт тусгайлан авч үзэх шаардлагатай.

Түвшин: дунд

Сэргийлэх арга хэмжээ

Лог Бүртгэл

ASD-ийн ACSC-ийн шалгалтын үеэр нийтлэг тулгардаг асуудлуудын нэг нь веб серверийн хүсэлт, Windows үйл явдлын бүртгэл болон интернет прокси бүртгэл зэрэг олон талын бүрэн бүтэн, түүхэн мэдээлэл хангалтгүй байдал нь мөрдлөгийн үр дүн болон хурдыг бууруулдаг.

ASD-ийн ACSC нь Windows үйл явдлын бүртгэл ба дамжуулалтын удирдамжийг харгалзан үзэж, хэрэгжүүлэхийг зөвлөж байна. Үүнд Windows үйл явдлын бүртгэлийн агуулах дахь тохиргооны файлууд болон скриптүүд, мөн Мэдээллийн Аюулгүй Байдлын Гарын Авлагын Системийн Хяналтын Зааварчилгаа багтана. Түүнчлэн бүртгэлийг төвлөрүүлэн хадгалах, тохиромжтой хугацаагаар хадгалах зохистой арга хэмжээг авахыг зөвлөж байна.

Шинэчлэлтийн менежмент

Интернэтэд холбогдох бүх төхөөрөмж, үйлчилгээ, үүнд веб серверүүд, веб аппликейшнүүд, Зайн хандалтын гарцуудыг яаралтай шинэчлэхийг зөвлөж байна. Шинэчлэлтийн процессыг автоматжуулж түргэсгэхийн тулд төвлөрсөн шинэчлэлтийн менежментийн систем нэвтрүүлэхийг санал болгож байна. ASD-ийн ACSC нь Мэдээллийн Аюулгүй Байдлын Гарын Авлагын (Системийн Удирдлагын Зааварчилгаа) ялангуяа Системийн Шинэчлэлтийн хяналтуудыг хэрэгжүүлэхийг зөвлөж байна.

Халдагч этгээдүүд ихэвчлэн олон нийтэд ил болсон, шинэчлэлт эсвэл хамгаалалтын арга хэмжээтэй сул талыг ашигласан байдаг. Байгууллагууд нь интернэтэд шууд холбогддог дэд бүтцэд 48 цагийн дотор аюулгүй байдлын шинэчлэлт эсвэл хамгаалалтыг хэрэгжүүлсэн байх шаардлагатай бөгөөд боломжтой тохиолдолд программ хангамж болон үйлдлийн системүүдийн хамгийн сүүлийн үеийн хувилбарыг ашиглахыг зөвлөж байна.

Сүлжээний сегментчлэл

Сүлжээний сегментчлэл нь халдагч этгээдүүдийг байгууллагын хувийн, нууц мэдээлэлд хүрэх боломжийг эрс хязгаарлаж чадна. Сүлжээг хэсэгчилснээр шаардлагагүй бол компьютер хоорондын холболтыг хязгаарлаж, дамжин шилжилтийн халдлагын (lateral movement) зогсоох боломжтой. Чухал серверүүд, жишээ нь Active Directory болон бусад баталгаажуулалтын серверүүд зөвхөн цөөн тооны завсрын сервер буюу ‘jump server’-ээс удирдлагатай байх ёстой. Эдгээр серверүүдийг нарийн хянаж, сайтар хамгаалж, ямар хэрэглэгч, төхөөрөмжүүд холбогдохыг хатуу хязгаарлах хэрэгтэй.

Хэдийгээр дамжин шилжилтийн халдлагыг зарим тохиолдолд зогсоосон ч, сүлжээний нэмэлт сегментчлэл нь халдагчдын хандаж чадах мэдээллийн хэмжээг илүү хязгаарлах боломжтой байв.

Нэмэлт сэргийлэх арга хэмжээнүүд

APT40 болон бусад халдагч этгээдийн хэрэглэж буй TTP (тактик, техник, үйл явц)-ийн эсрэг дараах нэмэлт арга хэмжээг зохих байгууллагууд зөвлөж байна:

- Хэрэглэгддэггүй эсвэл шаардлагагүй сүлжээний үйлчилгээ, порт, протоколуудыг идэвхгүй болгох.
- Веб сервер, аппликейшнүүдийг хамгаалахын тулд сайн тохиргоотой Веб Аппликейшн хамгаалалт (WAF) ашиглах.
- Сервер, файлын хуваалтууд болон бусад нөөцөд хандах эрхийг хамгийн бага эрхээр (least privilege) хязгаарлах.
- Нэвтрэлтүүдийг илүү бат бөх, дахин ашиглахад хэцүү болгохын тулд давхар баталгаажуулалт (MFA) болон удирдлагатай үйлчилгээний аккаунтыг ашиглах. MFA-г интернэтэд холбогддог зайнаас нэвтрэлтийн бүх үйлчилгээ заавал хэрэгжүүлэх шаардлагатай, үүнд:
  - Веб болон үүлэн суурьтай имэйл
  - Хамтын ажиллагааны платформууд
  - Хувийн виртуал сүлжээний (VPN) холболтууд
  - Зайн Десктоп үйлчилгээ (Remote Desktop Services)
- Ашиглалтын хугацаа нь дууссан тоног төхөөрөмжийг шинэчлэх шаардлагатай.

Хүснэгт 1: Сэргийлэх стратеги/Техникүүд

TTP	Нэн шаардлагатай найман хамгаалалтын стратеги	ISM хяналтууд
Эхний нэвтрэлт T1190 Нийтийн хандалттай веб програмыг ашиглан нэвтрэх	Програм хангамжийн шинэчлэлэлт Үйлдлийн системийн шинэчлэлэлт Давхар баталгаажуулалт Аппликейшн хяналт	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Гүйцэтгэл T1059 Комманд болон Скрипт Интерпретэр	Аппликэйшн хяналт Microsoft Office макро-г хязгаарлах Админ эрхийг хязгаарлах	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Тогтвортой нэвтрэх байдал (Persistence) T1505.003 Серверийн програмын бүрэлдэхүүн хэсэг: Арын хаалга (Web Shell)	Аппликейшн хяналт Админ эрхийг хязгаарлах	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Анхны хандалт / Эрхийн өргөлт / Тогтвортой нэвтрэх байдал T1078 Хүчин төгөлдөр хэрэглэгчийн бүртгэл ашиглах	Үйлдлийн системд шинэчлэлт хийх Давхар баталгаажуулалт Админ эрхийг хязгаарлах Аппликейшн хяналт Хэрэглэгчийн аппликейшнийг сайжруулах	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

MITRE ATT&CK техникийн хуудас дээрх “Mitigations” ба “Detection” хэсгүүдийг ашиглан энэ зөвлөмжийн төгсгөлд дурдсан MITRE ATT&CK техникийн зааварчилгааны дагуу тус бүрт тохирсон илрүүлэлт, хамгаалалтын арга хэмжээтэй танилцана уу.

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү тайланд багтсан мэдээллийг зөвхөн мэдээллийн зориулалтаар, “байгаагаар нь” хүргэж байна. Уг баримт бичигт дурдагдсан аливаа аж ахуйн нэгж, бүтээгдэхүүн, компани эсвэл үйлчилгээ, мөн энэ баримт бичигт холбоосоор дурдагдсан аливаа хуулийн этгээд, бүтээгдэхүүн, үйлчилгээг хэрэглэхийг сурталчилж буй хэрэг биш гэдгийг анхаарна уу. Тодорхой арилжааны байгууллага, бүтээгдэхүүн, үйл явц эсвэл үйлчилгээг нэр заасан нь (үйлчилгээний тэмдэг, худалдааны тэмдэг, үйлдвэрлэгч гэх мэтээр) зохиогч агентлагуудын зүгээс дэмжиж байна, зөвлөж байна гэсэн утгатай биш юм.

Энэхүү баримт бичгийг TLP:CLEAR гэж тэмдэглэсэн болно. Түгээхэд хязгаарлалтгүй. TLP:CLEAR ангилалтай мэдээлэл нь нийтэд нээлттэй хэвлэгдэн гарах дүрэм журамд нийцсэн, буруугаар ашиглах магадлал багатай үед хэрэглэгддэг. Стандарт зохиогчийн эрхийн дүрмийн дагуу, TLP:CLEAR мэдээллийг ямар нэг хязгаарлалтгүйгээр түгээж болно. Гэрлэн дохионы протокол (TLP)-ын талаар дэлгэрэнгүй мэдээллийг дараах хаягаас авна уу: cisa.gov/tlp

MITRE ATT&CK – APT40 бүлгийн түүхэн халдлагын аргачлалын сонирхолтой баримтууд

Мэдээлэл тандан цуглуулалах (Reconnaissance) (TA0043)	
Хохирогчийн эзэмшлийн веб сайтуудад хайлт хийх (T1594)	Хохирогчийн хувийн мэдээлэл цуглуулах: Нэвтрэх нэр, нууц үг (Credentials) (T1589.001)
Идэвхтэй хайлт хийн шалгах: Сул талыг хайлт хийх (T1595.002)	Хохирогчийн хостын мэдээлэл цуглуулах (T1592)
Нээлттэй вебсайт/домэйн хайх: Хайлтын системүүд ашиглах (T1593.002)	Хохирогчийн сүлжээний мэдээлэл цуглуулах: Домэйн шинж чанарууд (T1590.001)
Хохирогчийн хувийн мэдээлэл цуглуулах: Имэйл хаягууд (T1589.002)	

Нөөц хөгжүүлэлт (Resource Development) (TA0042)	
Дэд бүтцийг олж авах: Домэйн нэр (T1583.001)	Дэд бүтцийг (T1583) олж авах:
Дэд бүтцийг олж авах: DNS сервер (T1583.002)	Хаягийг хяналтандаа авах (T1586)
Чадварыг хөгжүүлэх: Кодын гарын үсгийн гэрчилгээ (T1587.002)	Дэд бүтцийг хяналтандаа авах (T1584)
Чадварыг хөгжүүлэх: Дижитал гэрчилгээ (T1587.003)	Чадварыг хөгжүүлэх: Хортой програм хангамж (Malware) (T1587.001)
Чадвар олж авах: Кодын гарын үсгийн гэрчилгээ (T1588.003)	Аккаунт үүсгэх: Үүлэн аккаунтууд (Cloud Accounts) (T1585.003)
Дэд бүтцийг хяналтандаа авах: Сүлжээний төхөөрөмжүүд (T1584.008)	Чадвар олж авах: Дижитал гэрчилгээ (T1588.004)

Эхний нэвтрэлт (TA0001)	
Хүчин төгөлдөр хаягууд (T1078)	Фишинг (T1566)
Хүчин төгөлдөр хаягууд: Анхдагч хаягууд (Default Accounts) (T1078.001)	Фишинг: И-мэйл хавсаргалт ашигласан фишинг (Spearphishing Attachment) (T1566.001)
Хүчин төгөлдөр хаягууд: Домэйн хаягууд (Domain Accounts) (T1078.002)	Фишинг: И-мэйл холбоос ашигласан фишинг (Spearphishing Link) (T1566.002)
Гадны алсын үйлчилгээ (External Remote Services) (T1133)	Нийтийн хандалттай програмд халдах (Exploit Public-Facing Application) (T1190)
Тусгай сайт руу халдах (Drive-by Compromise) (T1189)	

Гүйцэтгэл (TA0002)	
Windows удирдлагын багаж (Windows Management Instrumentation) (T1047)	Комманд ба скрипт тайлбарлагч: Python (T1059.006)
Төлөвлөсөн даалгавар/ажил: At (T1053.002)	Комманд ба скрипт тайлбарлагч: JavaScript (T1059.007)
Төлөвлөсөн даалгавар/ажил: Төлөвлөсөн даалгавар (Scheduled Task) (T1053.005)	Төрөлх API (Native API) (T1106)
Комманд ба скрипт тайлбарлагч (T1059)	Процесс хоорондын харилцаа (Inter-Process Communication) (T1559)
Комманд ба скрипт тайлбарлагч: Windows командын арын хаалга (Windows Command Shell) (T1059.003)	Системийн үйлчилгээ: Үйлчилгээ гүйцэтгэх (Service Execution) (T1569.002)
Комманд ба скрипт тайлбарлагч: PowerShell (T1059.001)	Үйлчлүүлэгч гүйцэтгэлийн ашиглалт (Exploitation for Client Execution) (T1203)
Комманд ба скрипт тайлбарлагч: Visual Basic (T1059.005)	Хэрэглэгчийн гүйцэтгэл: Хортой файл (Malicious File) (T1204.002)
Комманд ба скрипт тайлбарлагч: Unix Shell (T1059.004)	Комманд ба скрипт тайлбарлагч: Apple Script (T1059.002)
Төлөвлөсөн даалгавар/ажил: Cron (T1053.003)	Програм хангамж тараах хэрэгслүүд (Software Deployment Tools) (T1072)

Тогтвортой нэвтрэлт хийх (TA0003)	
Хүчин төгөлдөр хаягууд (T1078)	Серверийн програм хангамжийн бүрэлдэхүүн: Арын хаалга (Web Shell) (T1505.003)
Office програм эхлүүлэх: Office загвар макро (Office Template Macros) (T1137.001)	Систем процесс үүсгэх эсвэл засварлах: Windows үйлчилгээ (Windows Service) (T1543.003)
Төлөвлөсөн ажил: At (T1053.002)	Системийн ачаалалт буюу нэвтрэх үед автоматаар гүйцэтгэл: Бүртгэлийн гүйцэтгэлийн түлхүүрүүд / Эхлүүлэх хавтас (Registry Run Keys / Startup Folder) (T1547.001)
Төлөвлөсөн даалгавар/ажил: Төлөвлөсөн даалгавар (Scheduled Task) (T1053.005)	Ачаалалт буюу нэвтрэлтийн автоматаар эхлүүлэх гүйцэтгэл: Товчлол засварлах (Shortcut Modification) (T1547.009)
Гадны зайн үйлчилгээ (External Remote Services) (T1133)	Гүйцэтгэлийн урсгалыг булаах: DLL хайлтын дарааллын булаалт (DLL Search Order Hijacking) (T1574.001)
Төлөвлөсөн даалгавар/ажил: Cron (T1053.003)	Гүйцэтгэлийн урсгалыг булаах: DLL хажуугийн ачаалалт (DLL Side-Loading) (T1574.002)
Дансны удирдлага (Account Manipulation) (T1098)	Хүчин төгөлдөр хаягууд: Үүлэн хаягууд (Cloud Accounts) (T1078.004)
Хүчин төгөлдөр хаягууд: Домэйн хаягууд (Domain Accounts) (T1078.002)	

Нэвтрэх эрх нэмэгдүүлэх (Privilege Escalation) (TA0004)	
Төлөвлөсөн даалгавар/ажил: At (T1053.002)	Систем процесс үүсгэх эсвэл засварлах: Windows үйлчилгээ (Windows Service) (T1543.003)
Төлөвлөсөн даалгавар/ажил: Төлөвлөсөн даалгавар (Scheduled Task) (T1053.005)	Ачаалалт буюу нэвтрэлтийн автоматаар эхлүүлэх гүйцэтгэл: Бүртгэлийн гүйцэтгэлийн түлхүүрүүд / Эхлүүлэх хавтас (Registry Run Keys / Startup Folder) (T1547.001)
Процесс шингээлт: Утсан гүйцэтгэлийг булаах (Thread Execution Hijacking) (T1055.003)	Ачаалалт буюу нэвтрэлтийн автоматаар эхлүүлэх гүйцэтгэл: Товчлол засварлах (Shortcut Modification) (T1547.009)
Процесс шингээлт: Процесс хооглох (Process Hollowing) (T1055.012)	Гүйцэтгэлийн урсгалыг булаах: DLL хайлтын дарааллын булаалт (DLL Search Order Hijacking) (T1574.001)

Нэвтрэх эрх нэмэгдүүлэх (Privilege Escalation) (TA0004)	
Хүчин төгөлдөр хаягууд: Домэйн хаягууд (Domain Accounts) (T1078.002)	Нэвтрэх эрх нэмэгдүүлэх зорилгоор ашиглах (Exploitation for Privilege Escalation) (T1068)
Нэвтрэх тэмдгийн удирдлага: Тэмдэг дууриалган хулгайлах (Token Impersonation/Theft) (T1134.001)	Үйл явдалд өдөөгдсөн гүйцэтгэл: Unix Shell тохиргооны засвар (Unix Shell Configuration Modification) (T1546.004)
Процесс шингээлт: Динамик холболтын номын сангийн шингээлт (Dynamic-link Library Injection) (T1055.001)	Хүчин төгөлдөр хаягууд: Домэйн хаягууд (Domain Accounts) (T1078.002)
Хүчин төгөлдөр хаягууд: Локал хаягууд (Local Accounts) (T1078.003)	

Хамгаалалт тойрч гарах (Defence Evasion) (TA0005)	
Rootkit (T1014)	Шууд бус комманд гүйцэтгэл (Indirect Command Execution) (T1202)
Нууцлагдсан файлууд эсвэл мэдээлэл (Obfuscated Files or Information) (T1027)	Системийн бинарийн төлөөлөгч гүйцэтгэл: Mshta (T1218.005)
Нууцлагдсан файлууд эсвэл мэдээлэл: Програм хангамж боох (Software Packing) (T1027.002)	Системийн бинарийн төлөөлөгч гүйцэтгэл: Regsvr32 (T1218.010)
Нууцлагдсан файлууд эсвэл мэдээлэл: Стеганографи (Steganography) (T1027.003)	Subvert Trust хяналт: Код гарын үсэг (Code Signing) (T1553.002)
Нууцлагдсан файлууд эсвэл мэдээлэл: Хүргэлтийн дараа нэгтгэх (Compile After Delivery) (T1027.004)	Файл ба хавтасны эрхийн өөрчлөлт: Linux ба Mac файл, хавтасны эрх өөрчлөлт (T1222.002)
Хуулбарлан дуурайх: Хүчин төгөлдөр нэр эсвэл байршилтай таарах (Match Legitimate Name or Location) (T1036.005)	Виртуалжуулалт / Сандбокс тойрч гарах: Системийн шалгалтууд (System Checks) (T1497.001)
Процесс шингээлт: Утсан гүйцэтгэлийг булаах (Thread Execution Hijacking) (T1055.003)	Хуулбарлан дуурайх (T1036)
Тусгай код ачаалалт (Reflective Code Loading) (T1620)	Хамгаалалтыг сулруулах: Системийн гал хамгаалалтыг унтраах эсвэл өөрчлөх (Disable or Modify System Firewall) (T1562.004)
Процесс шингээлт: Процесс хоослох (Process Hollowing) (T1055.012)	Баталгааг нуух: Нуугдсан файлууд ба хавтаснууд (Hidden Files and Directories) (T1564.001)
Үзүүлэлтийг арилгах: Файл устгах (File Deletion) (T1070.004)	Баталгааг нуух: Нуугдсан цонх (Hidden Window) (T1564.003)
Үзүүлэлтийг арилгах: Цаг хугацааны өөрчлөлт (Timestomp) (T1070.006)	Гүйцэтгэлийн урсгалыг булаах: DLL хайлтын дарааллын булаалт (DLL Search Order Hijacking) (T1574.001)
Үзүүлэлтийг арилгах: Windows үйл явдлын бүртгэлийг цэвэрлэх (Clear Windows Event Logs) (T1070.001)	Гүйцэтгэлийн урсгалыг булаах: DLL хажуугийн ачаалалт (DLL Side-Loading) (T1574.002)
Бүртгэлийг засах (Modify Registry) (T1112)	Вэб үйлчилгээ (Web Service) (T1102)
Файлууд эсвэл мэдээллийг тайлах/код задлах (Deobfuscate/Decode Files or Information) (T1140)	Хуулбарлан дуурайх: Хуулбарлан дуурайх даалгавар эсвэл үйлчилгээ (T1036.004)
Хамгаалалтыг сулруулах (Impair Defenses) (T1562)	

Нууцлалын мэдээлэл авах (Credential Access) (TA0006)	
OS-н нууцлалын мэдээлэл хуулбарлах: LSASS санах ой (LSASS Memory) (T1003.001)	Хамгаалалтгүй нууцлалын мэдээлэл: Файлуудад хадгалагдсан нууцлал (Credentials in Files) (T1552.001)
OS-н нууцлалын мэдээлэл хуулбарлах: NTDS (T1003.003)	Нууц үгийн халдлагын арга: Нууц үг таах (T1110.001)
Сүлжээний тагналт (T1040)	Албадан баталгаажуулалт (T1187)

Нууцлалын мэдээлэл авах (Credential Access) (TA0006)	
Нууц үг хадгалах сангаас мэдээлэл хулгайлах: Keychain (T1555.001)	Kerberos тасалбарыг хулгайлах эсвэл хуурамчаар үйлдэх: Kerberoasting (T1558.003)
Ороолт бүртгэх: Гарны бичлэг хийх (T1056.001)	Олон хүчин зүйлт баталгаажуулалтыг саатуулах (T1111)
Веб хандалтын күүкийг хулгайлах (T1539)	Аппликейшний нэвтрэх токен хулгайлах (T1528)
Нэвтрэх мэдээлэлд халдах зорилготой эмзэг байдал ашиглалт (T1212)	Нууц үгийн халдлагын арга: Нууц үг тайлах (T1110.002)
Ороолт бүртгэх: Веб порталаас мэдээлэл авах (T1056.003)	Үйлдлийн системийн эрхтэй мэдээлэл хуулах: DCSync (T1003.006)
Нууц үг хадгалах сангаас эрх хулгайлах (T1555)	Нууц үг хадгалах сангаас мэдээлэл авах: Веб хөтөчөөс нууц үг хулгайлах (T1555.003)

Илрүүлэлт (TA0007)	
Системийн үйлчилгээ илрүүлэх (T1007)	Системийн мэдээлэл илрүүлэх (T1082)
Програмын цонх илрүүлэх (T1010)	Хаяг илрүүлэх: Локал хэрэглэгчийн хаяг (T1087.001)
Бүртгэл асуух (T1012)	Системийн мэдээлэл илрүүлэх, T1082 аргачлал – Байгууллага | MITRE ATT&CK®
Файл болон хавтас илрүүлэх (T1083)	Системийн цаг илрүүлэх (T1124)
Сүлжээний үйлчилгээ илрүүлэх (T1046)	Системийн эзэмшигч / хэрэглэгч илрүүлэх (T1033)
Алсаас систем илрүүлэх (T1018)	Домэйн итгэлцлийн харилцаа илрүүлэх (T1482)
Хаяг илрүүлэх: Имэйл хаяг (T1087.003)	Хаяг илрүүлэх: Домэйн хаяг (T1087.002)
Системийн сүлжээний холболт илрүүлэх (T1049)	Виртуал орчин болон хамгаалалт тойрох: Систем шалгах (T1497.001)
Үйл явц илрүүлэх (T1057)	Програм хангамж илрүүлэх (T1518)
Эрхийн бүлэг илрүүлэх: Домэйн бүлгүүд (T1069.002)	Сүлжээний Хуваалцах Нөөц Илрүүлэх, Техник T1135 - Байгууллага | MITRE ATT&CK®
Системийн сүлжээний тохиргоо илрүүлэх: Интернэт холболт илрүүлэх (T1016.001)	

Хажуугийн хөдөлгөөн (TA0008)	
Алсын үйлчилгээ: Remote Desktop Protocol (T1021.001)	Алсын үйлчилгээ (T1021)
Алсын үйлчилгээ: SMB/Windows админ хуваалт (T1021.002)	Өөр төрлийн баталгаажуулалтын мэдээлэл ашиглах: Тасалбар дамжуулах (Pass the Ticket) (T1550.003)
Алсын үйлчилгээ: Windows Remote Management (T1021.006)	Хажуугийн хэрэгслийн шилжүүлэлт (T1570)

Мэдээлэл цуглуулалт (TA0009)	
Локал системээс мэдээлэл цуглуулах (T1005)	Цуглуулсан мэдээллийг архивлах: Сангаар дамжуулан архивлах (T1560.002)
Сүлжээний хуваалцсан дискны мэдээлэл (T1039)	Имэйл цуглуулалт: Алсын имэйл цуглуулах (T1114.002)

Цуглуулга (TA0009)	
Ороолт Барих: Keylogging (T1056.001)	Хуулбарын өгөгдөл (Clipboard Data) (T1115)
Автоматжуулсан цуглуулга (Automated Collection) (T1119)	Мэдээллийн агуулахуудын өгөгдөл (Data from Information Repositories) (T1213)
Ороолт Барих: Веб портал дээрх баримт авах (Web Portal Capture) (T1056.003)	Өгөгдөл бэлтгэх: Алсын өгөгдөл бэлтгэх (Remote Data Staging) (T1074.002)
Өгөгдөл бэлтгэх: Локал өгөгдөл бэлтгэх (Local Data Staging) (T1074.001)	Цуглуулсан өгөгдлийг архивлах (Archive Collected Data) (T1560)
Имэйл цуглуулах (Email Collection) (T1114)	

Мэдээлэл гадагш хулгайлах (Exfiltration) (TA0010)	
Команд удирдлагын сувгаар хулгайлах (Exfiltration Over C2 Channel) (T1041)	Өөр протокол ашиглан хулгайлах: Тэгш бус шифрлэгдсэн, C2 биш протокол ашиглах гадагшлуулах (Exfiltration Over Asymmetric Encrypted Non-C2 Protocol) (T1048.002)
Өөр протокол ашиглах хулгайлах (Exfiltration Over Alternative Protocol) (T1048)	Веб үйлчилгээ ашиглан хулгайлах: Үүлэн хадгалах сан руу хулгайлах (Exfiltration to Cloud Storage) (T1567.002)

Команд ба Удирдлага (TA0011)	
Өгөгдөл нуух (Data Obfuscation): Протокол хуурамчаар үйлдэх (Protocol Impersonation) (T1001.003)	Веб үйлчилгээ: Dead Drop Resolver (T1102.001)
Түгээмэл ашиглагддаг порт (Commonly Used Port) (T1043)	Веб үйлчилгээ: Нэг чиглэлийн харилцаа (One-way Communication) (T1102.003)
Аппликейшний үечлэлийн протокол: Веб протоколууд (Web Protocols) (T1071.001)	Хэрэгсэл шилжүүлэх (Ingress Tool Transfer) (T1105)
Аппликейшний үечлэлийн протокол: Файл дамжуулах протоколууд (File Transfer Protocols) (T1071.002)	Прокси: Дотоод прокси (Internal Proxy) (T1090.001)
Прокси: Гаднах прокси (External Proxy) (T1090.002)	Стандарт бус порт (Non-Standard Port) (T1571)
Прокси: Олон шат дамжуулагч прокси (Multi-hop Proxy) (T1090.003)	Протокол туннелл хийх (Protocol Tunnelling) (T1572)
Веб үйлчилгээ: Хоёр чиглэлийн харилцаа (Bidirectional Communication) (T1102.002)	Шифрлэгдсэн сувгаар дамжуулах (Encrypted Channel) (T1573)
Шифрлэгдсэн сувгаар дамжуулах: Тэгш бус криптографи (Asymmetric Cryptography) (T1573.002)	Хэрэгсэл шилжүүлэх (Ingress Tool Transfer) (T1105)
Прокси, Техник T1090 - Байгууллага | MITRE ATT&CK®	

Нөлөөлөл (TA0040)	
Үйлчилгээг зогсоох (Service Stop) (T1489)	Диск устгах (Disk Wipe) (T1561)
Системийг унтраах/дахин ачаалах (System Shutdown/ Reboot) (T1529)	Ресурсыг булаан авах (Resource Hijacking) (T1496)

Тэмдэглэлүүд

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү гарын авлагын материал нь ерөнхий агуулгатай бөгөөд хууль зүйн зөвлөгөө гэж үзэхгүй бөгөөд тодорхой нөхцөл байдал эсвэл яаралтай үед тусламж авахад түшиглэх ёсгүй болно. Ямар нэгэн чухал асуудал үүссэн бол өөрийн нөхцөл байдалд зохисон, бие даасан мэргэжлийн зөвлөгөөг авахыг зөвлөж байна.

Энэхүү гарын авлагад агуулагдсан мэдээлэлд үндэслэн хийсэн аливаа үйлдлээс улбаалсан аливаа хохирол, алдагдал, зардлыг Холбооны улс хариуцахгүй.

Зохиогчийн эрх

Төрийн сүлдийг ашиглах эрх

Төрийн сүлдийг ашиглах нөхцөлийн талаарх дэлгэрэнгүй мэдээлэл болон зааврыг Ерөнхий сайд ба Засгийн газрын Тамгын газрын вебсайт Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au дээрээс авна уу.

Дэлгэрэнгүй мэдээлэл авах эсвэл кибер аюулгүй байдлын тохиолдлыг мэдээлэх бол бидэнтэй холбогдоно уу:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Энэ дугаарыг зөвхөн Австралийн дотор ашиглах боломжтой.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre