セキュリティ総論 D レポート No.4

慶應義塾大学 61908697 佐々木良輔

1　セキュリティ事故調査

1.1　年金管理システムサイバー攻撃

1.1.1　概要

2015 年 5 月に特殊法人 日本年金機構の職員個人端末がマルウェアに感染し 125 万件の個人情報が流出した.

1.1.2　要因

攻撃は標的型攻撃メールによって行われた. 5 名の職員がこのメールを開封し, それぞれの利用端末がマルウェアに感染した. 攻撃に使用されたマルウェアは EMDIVI と呼ばれるもので, PDF などに偽装された実行ファイルによってインストールされ, 感染した PC は外部のサーバーを介してリモート操作される.[1] これによって端末から個人情報が流出した.[2]

1.1.3　被害組織の対応

最初に組織が事案を認識したのは 5 月 8 日に NISC によって「不審な通信を検知」という通報がなされたときであり, 組織は当該端末の抜線を行った. しかし組織内での情報共有や標的型攻撃メールに対する注意喚起が不十分であり, またメールアドレスの受信拒否設定や URL フィルタリングを行わなかった. したがって 5 月 21 日には再び標的型攻撃メールが開封され, 個人情報が流出するに至った. またインシデント時の対応に関するルールがなく, 組織全体でのインターネット遮断などの対応が遅れたことも被害の拡大の原因である. このことから事案を認識していたにも関わらず対応が不十分であったために被害が拡大したと言える. このインシデントを受けて日本年金機構ではお客様対応として相談窓口の設置, また機構 CSIRT の設置やガバナンスの改革, セキュリティポリシーの改正などを行った.[2]

1.1.4　考察

最初に事案を認識した 5 月 8 日時点では個人情報の流出は起こっておらず, 業務用メールアドレスが漏洩しただけだった. したがって巧妙な標的型攻撃メールを完全に防御することは困難だとしても, 最初に事案を認識した時点で適切な対応をしていれば 125 万件の個人情報流出は防げたと考

えられる．このためには組織内での情報共有やセキュリティに関する教育を徹底するべきだと考えられる．

1.2 Aurora 作戦

1.2.1 概要

2010 年 1 月 12 日に Google がサイバー攻撃を受けたことを発表した. 攻撃は中華人民共和国の Elderwood グループなどによって行われたと考えられており, Google の他に 20 社程度の米企業が攻撃を受けたと言われている.[3]

1.2.2 要因

攻撃は高度な (Advanced), 執拗な (Persistent), 脅威 (Threat) の頭文字を取った APT 攻撃という手法で行われ標的型攻撃の一種である．攻撃には Internet Explorer の Use-after-free 脆弱性 (CVE-2010-0249) が用いられており, 脆弱性はパッチの当てられていない Windows 2000 SP4, Windows XP, Windows 7 などの OS に存在するものである.[4] この脆弱性は攻撃が行われた当時公開されておらず, ゼロデイ攻撃であった．攻撃は Exploit を仕込まれた PDF が添付された標的型攻撃メールによって行われたと考えられている．これによって端末にバックドアが仕込まれ, Gmail のアカウントなどに不正アクセスされた.

1.2.3 被害組織の対応

Microsoft はこの脆弱性に対して更新プログラムを公開し, これを適用することで脆弱性を解消できる.[5] また Google はこれを受けて中国本土でのネット検索サービスから撤退し, 中国からのアクセスを香港のサーバーに転送することとした.

1.2.4 考察

この事例はゼロデイ攻撃であったため, 対策は難しいと考えられる．したがってこういった攻撃に備えるには常にパッチや更新プログラムを当てること, また可能であれば不審な通信を監視することが必要だと考えられる．また近年では国家によるサーバー攻撃が増加しており, 防衛も国家として行う必要があると考えられる.

1.3 本田技研工業の WannaCry 感染

1.3.1 概要

2017 年 6 月 18 日に本田技研工業の工場などの拠点で生産ラインの管理などに用いる端末がランサムウェアに感染し, 生産ラインが影響を受けた.[6]

1.3.2 要因

攻撃にはランサムウェアである WannaCry が用いられている．WannaCry は Windows のネットワークでのファイル共有プロトコルである SMBv1 の不適切な入力確認によるリモートコード実行脆弱性 (CVE-2017-0143) を用いてバックドアを作成し, 感染を広げるものである．この脆弱性は Windows Vista から Windows 10 までのコンシューマー向け OS や Windows Server 2008 から Windows Server 2016 までのサーバー向け OS など幅広い OS に存在する.[7] しかし 2017 年 3 月 14 日時点でセキュリティパッチが公開されており, パッチが当たっていない Windows 7 への感染が多かった．感染した PC にはセキュリティパッチが当たっておらず, 脆弱性があったために感染したとされている.[6]

1.3.3 被害組織の対応

本田技研工業では各拠点に対して WannaCry の注意喚起を行っていたため, 感染した PC は直ちにネットワークから隔離した．対応が早かったため感染の拡大や生産ラインへの大きな影響はなかった.[6]

1.3.4 考察

この事案では組織内で注意喚起がされており, 直ぐに感染源を隔離できた．一方で WannaCry により大きな影響を受けた組織は多く存在した．たとえばイギリスでは国民保険サービスのシステムが感染し, 一部病院が閉鎖されることもあった.[8] 本田技研工業の事例について, 具体的にどのような PC が感染したのかは公表されていないが, 工場設備に付帯する PC ということから FA 機器などの制御用端末と考えられる．こういった PC は更新が困難であるから, 基本的には常にネットワークから遮断する, あるいはネットワーク接続が必要な場合は境界防御やアンチウイルスソフトウェアの導入が必要だと考えられる．

参考文献

[1] ASCII.jp.「emdivi」使い多発する日本への標的型攻撃. https://ascii.jp/elem/000/001/019/1019316/, 6 2015. (Accessed on 12/22/2021).

[2] 日本年金機構. 不正アクセスによる情報流出事案に関する調査結果報告について. https://www.nenkin.go.jp/info/index.files/e7wRRjRfiKiN1.pdf, 8 2015. (Accessed on 12/22/2021).

[3] Operation aurora - wikipedia. https://en.wikipedia.org/wiki/Operation_Aurora. (Accessed on 12/22/2021).

[4] NIST. Cve-2010-0249 - national vulnerability database. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249. (Accessed on 12/22/2021).

[5] Microsoft. Microsoft security advisory 979352. https://docs.microsoft.com/

ja-jp/security-updates/securityadvisories/2010/979352, 1 2010. (Accessed on 12/22/2021).

[6] 井上英明. ホンダが工場など複数拠点で wannacry 感染、一部の生産に影響. https://xtech.nikkei.com/it/atcl/news/17/062101713/, 6 2017. (Accessed on 12/22/2021).

[7] JVN iPedia. Jvndb-2017-001842. https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-001842.html. (Accessed on 12/22/2021).

[8] 原口 昇平 Shona Ghosh. 英国でも猛威 windows xp でランサムウェア広まる. https://www.businessinsider.jp/post-33600, 3 2017. (Accessed on 12/22/2021).