

会員限定

2021年2月度合同研究会
金融マーケティング研究会
金融システム研究会
2021年2月8日～12日

Vol. 1 サイバーセキュリティは弱肉強食、強ければ生き弱ければ4ぬ

講師：守井 浩司

株式会社レオンテクノロジー 代表取締役社長

Vol. 2 攻撃者が認証突破に用いる方法とシステム側で実施すべき対策

講師：江ノ本 司

株式会社レオンテクノロジー 執行役員 技術統括本部長

EC-Council CEH (Certified Ethical Hacker : 認定ホワイトハッカー) 認定講師

CONTENTS

目次

Vol. 1 サイバーセキュリティは弱肉強食、強ければ生き弱ければ死ぬ

Vol. 2 攻撃者が認証突破に用いる方法とシステム側で実施すべき対策

第1部	4
Slide 1 自己紹介	4
Slide 2 今日伝えたい事	6
Slide 3 目次	6
第一章 攻撃者は御組織の強さと弱さをどう判断するのか?	8
Slide 5 第一章 始める前の余談 01	8
Slide 6 第一章 始める前の余談 02	10
Slide 7 第一章 だから攻撃者の目線で自社を見るのが大事	10
Slide 8 OSINT 利用について	12
Slide 9 攻撃段階ステップの説明	12
Slide 10 OSINT を利用して知ることができる範囲	14
Slide 11 サイバーキルチェーン7つのステップの説明	14
Slide 12 サイバーキルチェーン7つのステップの説明	16
Slide 13 OSINT で得られる情報例	16
Slide 14 自社でも OSINT を使ってみる	18
Slide 13 OSINT で得られる情報例	18
Slide 14 自社でも OSINT を使ってみる	18
第二章 ネットワーク分離やってますけど分離したイントラネットに侵入できるんですがの例	18
Slide 16 悪意ある第三者が攻撃する動機について	20
Slide 17 ①依頼主に依頼され標的として攻撃する(スポンサー型)	20
Slide 18 ②確実に金になる算段を取得し攻撃を実施する(ノンスポンサー型)	22
Slide 19 ③狙いやすかったから(攻撃成功期待度は高くはないものの狙う動機たる脆弱性などが存在する)	22
Slide 20 ④たまたま(たまたま標的型メール攻撃に引っ掛かったから等)	24
Slide 21 ⑤何となく w	24
Slide 22・23 悪意ある第三者が攻撃する動機について	26

Slide 24	攻撃段階ステップの説明	28
Slide 25 ~ 30	サイバークルチェーン7つのステップの説明	28
Slide 31	長い前振りでしたけども	34
Slide 31・32	攻撃者の偵察行為で情報を「渡さない」ことが大事	34
Slide 33	インターネット分離環境へ侵入するための手口	36
Slide34	昨今の内部情報が漏れてる場合の例	38
第三章	セキュリティソフトをすり抜けた悪意ある攻撃をどのように検知するのか?	38
Slide 36	被害に遭わない対策だけでは不十分	40
Slide 37	ログ取得と監視分析に求められる機能要件について	40
Slide 38	ありました、レオンのログ収集分析サービス	42
Slide 39	大流行の Emotet やランサムに感染するとどうなる?	42
Slide 40・41	ランサムに対して有用な予防策①②	44
Slide 42	今後課題となることが予想されるセキュリティの事柄	46
第2部		48
Slide 2	自己紹介	48
Slide 3	今回のテーマについて	50
Slide 4	目次	50
第一章	攻撃者はどのように認証情報を収集するのか	52
Slide 6	認証情報	52
Slide 7	① 利用者自身に入力させる(フィッシングサイト)	54
Slide 8	フィッシングサイトの対策とされるもの	54
Slide 9	② 既に漏洩している情報を買う(ダークウェブ)	56
Slide 10	ダークウェブ内で売られているもの	56
Slide 11	その他もろもろ	58
第二章	収集した情報を使ってどのような攻撃を仕掛けてくるのか	58
Slide 13	ログイン画面の突破方法	60
Slide 14	パスワードの推測方法 ①辞書攻撃	60
Slide 15	パスワードの推測方法 ②ブルートフォース	62
Slide 16	パスワードの推測方法 ③リバースブルートフォース	62

Slide 17	でもいざ実行しようとする	64
Slide 18	手に入れた情報を効率よく使おう	64
第三章	攻撃を防ぐために必要な認証の3大要素	66
Slide 20	認証の3要素	66
Slide 21	① 知識情報 (Something You Know)	68
Slide 22	② 所持情報 (Something You Have)	68
Slide 23	③ 生体情報 (Something You Are)	70
Slide 24	多要素認証	70
Slide 25	単要素にならないように	72
Slide 26	多要素認証で攻撃をブロック	72
Slide 27	多要素認証にも穴が存在します	74
Slide 28	多要素認証の穴 リアルタイムに攻撃された場合	74
Slide 29	多要素認証の穴 SMSを受信するスマホに不正なアプリがインストールされていた場合	76
第四章	脆弱な認証機構を作らない為のベストプラクティス	76
Slide 31	リアルタイムフィッシングの問題点	78
Slide 32	求められる実装	78
Slide 33	攻撃に対する対策	80
Slide 34	まとめ	80

第 1 部

ブンブンハロー YouTube !

はい、本日のテーマはですね、「サイバーセキュリティは弱肉強食。強ければ生き、弱ければ4ぬ」をテーマにお話をさしていただければと思います。

Slide 1 自己紹介

月並みですけども、「今年 40 歳の前厄ですがなにか?」ということですね、株式会社レオンテクノロジーの代表をやらしていただいております守井です。守井です!

ということで、ホワイトハッカーの育成と、まだまだ現場で診断やフォレンジックっていうサービス事業の対応もさしていただいておりますよということで、今年のテーマはですね、1 人でも多くのホワイトハッカーを生み出すというところに焦点を当てて活動中でございます。



『サイバーセキュリティは弱肉強食。強ければ生き、弱ければ4ぬ。』

株式会社レオンテクノロジー

2021年1月12日

Slide 1

代表取締役社長

守井 浩司/Koji Morii

1981年、京都府生まれ。株式会社レオンテクノロジー
2005年3月設立。

各種サイバーセキュリティ事業を展開。自身も現場の
最前線にて活動を続ける傍ら、ホワイトハッカー育成
やサイバーセキュリティの第一人者として、各種取材
や講演活動を通じて、セキュリティに関する啓蒙活動
に注力。

守井浩司



今年40歳の前厄ですがなにか？



Slide 2 今日伝えたい事

本日の「伝えたい事」っていうことですね、強さと弱さが指すものというのは、御組織が保有する機器を含めデジタル資産でございますよと。これらが外部からどのように見られているかというところのお話をさせていただきたいんですけども、まず、御社が一切公開したつもりがないシステム、既にこれらが、例えばどのようなシステムが運用されてて、どのようなバージョンで運用されてて、などの細かい情報が外部に漏れ出ていることってのがありますよと。

最近、往々にして、フォレンジックをさせていただくと、自社から漏れたものではなくて、外注先さんが漏らしたとか、既に漏れ出たものがある一定の期間放置された後に攻撃に転用されたとか、そういったことも多くございますので注意が必要ですよと、こういったところを、今日、一番強く言いたいところでございます。

本日、どのように情報が漏れ出たかではなくて、漏れ出た情報をどのように使って、攻撃のシナリオだったりとか、攻撃にどのように利用していくのかとかというところのお話をさせていただければということと、年末年始ですね、ランサムの感染で被害をお受けになった企業さんから調査の依頼というのがダーンと来たんですね。結構多かったんです。というところで、ランサムに対する警戒と、月並みなんですけども、どのように対応したらランサムからの感染を逃れられることができるのかというところについては、少し、最後のほうでお話しさせていただきたいと思えますし、本日の資料、最後のほうにその対策の内容とかが載っているんで、ぜひ御活用いただければということでございます。

では、早速。

Slide 3 目次

「攻撃者は御社の強さと弱さをどう判断するのか？」。

2 番目、「ネットワーク分離やってますけど、分離したイントラネットに侵入できるんですけど」という話ですね。

3 番は「セキュリティソフトをすり抜けた悪意ある攻撃をどのように検知する方法があるのか？」というところのお話です。

今日伝えたい事



- ◆ 強さと弱さが指すものは御組織が保有する機器を含むデジタル資産を指します。例えばインターネットに公開しているHPや自社で利用するシステム、社内NW環境や情報管理で利用している外部サービスや社内のファイルサーバーなど多岐に渡る御社保有の資産が対象です。
- ◆ 一切公開したつもりがない社内環境で利用している機器や保有資産をなぜ攻撃者が知り得ているのか？
御社から漏れたものでなくとも外注先やリモートワークなどで社外利用している端末や御社社内で利用するソフトウェアやNW設定から漏れ出ている可能性もあります。（※今日、これが一番言いたいこと）
- ◆ 今回はどのように情報が漏れるかではなく、漏れ出た情報や公開したつもりのない情報を攻撃者が利用しどのような攻撃シナリオで御社の重要資産や社内環境に潜り込むための手段とするのか？
の攻撃者目線の「調査方法」と「攻撃シナリオと手法」についてを解説します。

年始からランサムウェア感染の被害によるフォレンジックが多いので今年も去年に続きランサムウェアに対する警戒は必要です。つきなみですが対策内容も最後に掲載していきます。

Copyright © 2020 Leon Technology ,Inc.

2

目次



- 1 攻撃者は御組織の強さと弱さをどう判断するのか？
- 2 ネットワーク分離やってますけど分離したイントラネットに侵入できるんですがの例
- 3 セキュリティソフトをすり抜けた悪意ある攻撃をどのように検知するのか？

Copyright © 2020 Leon Technology ,Inc.

3

第一章 攻撃者は御組織の強さと弱さをどう判断するのか？

じゃ、まず第1章ね。「攻撃者は御組織の強さと弱さをどう判断するのか？」というところで、ちょっと余談です。

まずなんですけど、「コロナの影響で変わるハッカービジネス」というところをテーマにしています。

Slide 5 第一章 始める前の余談 01

まずコロナ前なんですけども、企業や国から依頼がたーんとございました、というところなんですけども、この中においては、やっぱりハッカービジネス、依頼が減少してきてます。そうすると、標的、つまり直接の金銭を早く得ないと自分たちの組織を維持することができないぞというところで、やっぱり金融機関だったりとか金融機関を利用するユーザーさん、これらをターゲットに攻撃を仕掛けてくる傾向にございますよというところで、こちら、1月の10日ぐらいですかにニュースにもなりましたが、フィッシングサイトがたくさんつくられてて、気いつけなはれや、っていうニュースだったりとか、ZeroLogonを使って侵入された後、重要な資産にたどり着いて情報を持っていかれるよ、なーんて脆弱性も発表されてたりなんかしています。

ちょっと、次、いきますね。

第一章

LEON TECHNOLOGY

攻撃者は御組織の強さと弱さをどう判断するのか？

Copyright © 2020 Leon Technology ,Inc.

4


第一章 始める前の余談01

LEON TECHNOLOGY

コロナの影響で「変わる」ハッカービジネス

- ・ コロナ前のハッカービジネス → 企業や国からの依頼が多い
- ・ コロナ禍でのハッカービジネス → 依頼が減少したり限定された標的への依頼となる。

多くのハッカー組織はクライアントからの依頼が減少したため即座に金銭を獲得しなければならない状況に陥っている
コロナ禍においては金融機関とその利用者を狙いダイレクトに金銭を搾取するための攻撃を実施し直接金銭を得たい思惑がある。



● 参照情報
<https://news.yahoo.co.jp/articles/0409475966d3662383672e77955a917fca37e>
<https://japan.zdnet.com/article/35160009/>

Copyright © 2020 Leon Technology ,Inc.

5

Slide 6 第一章 始める前の余談 02

「始める前の余談 02」です。

「より効率や成功期待値が高い攻撃を実施するために」というところで、一般的には調査という、後ほどお話をさしていただくんですけども、むやみやたらに攻撃することってめったにございません。なんですけども、当然、その事前に攻撃者も成功期待値の高い資産に対する攻撃を実施したいよというところで、その成功期待値を高いものを割り出すための調査を行うんですね。この調査っていうものが、いろんな方法はあるんですけども、SNS ですね、企業に所属する社員さんの SNS を利用したりとか、公式の、例えば企業のチャンネルや SNS を乗っ取ったり、それらを悪用したりというところで、情報を割り出したりとか、不透明な情報を透明化するというのもやるんですけども、これは非常に時間がかかるというところで、コロナ禍においては一刻一秒を争って金銭を略奪したいというところの目的で、既に情報が収集された OSINT を使って、攻撃の成功期待値の高いものから優先的に攻撃を仕掛けるという傾向がございますよと。

で、DX というキーワードで金融機関の皆様においても、クラウドサービスを活用したりとか、クラウド上のサービスを利用したりとかっていうことで、どんどん IT 化を推進されていると思います。

なんですけども、ちょっと考えてくださいよと。

利用するには、大きなメリットもございますけども、当然、デメリットというものもございますよと。

ていうところで、DX とかりモートワークとか、こういったキーワードが……このキーワードが流行るはるか以前から、守井さんは、DX といわれるもとかセキュリティ対策において取り組んできましたよと。なので、DX を成功に導くには守井さんの意見も取り入れたほうがうまくいくんじゃないか……っていうね……はい、そんな感じでございます。

Slide 7 第一章 だから攻撃者の目線で自社を見ることが大事

「だから攻撃者の目線で自社を見ることが大事」なんです、ってとこのお話です。

まずなんですけども、御社は攻撃者から御社のデジタル資産ですね、例えばホームページだったりとか社内ですべての PC 端末とか、それがどのように見られているか知ってますか？ってとこのお話です。

まずなんですけども、昨今の攻撃者は無作為に成

功確率が低い攻撃とかばらまき型の攻撃というのはあまりなくなってきましたよね、というお話は先ほどさしてもらいました。

なんですけども、「クライアントによる攻撃依頼」ってのがコロナ禍以前は多かったんですけども、それだけじゃなくて、「攻撃成功期待値の高い資産に対する攻撃」というのもやはり依然として実施されている傾向にありますし、あと、「わなに引っかけた人」ですね。フィッシングサイトもわなの一つなんですけども、例えばランサムだったりとか Emotet とか、最近でもウイルス、マルウェアですね、これらに感染した人の顔末だったりとか、その後、どのような事態に発展したかなんてことは皆さんも御存じかもしれません。

なんですけども、より成功期待値の高い資産に対する攻撃を実施するためにはやはり OSINT を使いますよというところ、さっきの繰り返しになってしまうんですけども、情報収集が済ませてしまっている OSINT を使って攻撃を仕掛ける傾向にありますよというところのお話でございます。