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

金財情報システム　研究会事務局

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 4 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

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！

ていうことで、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し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していただくと、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していただければというところと、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いますし、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ので、ぜひ御活用いただければというところでございます。

では、早速。

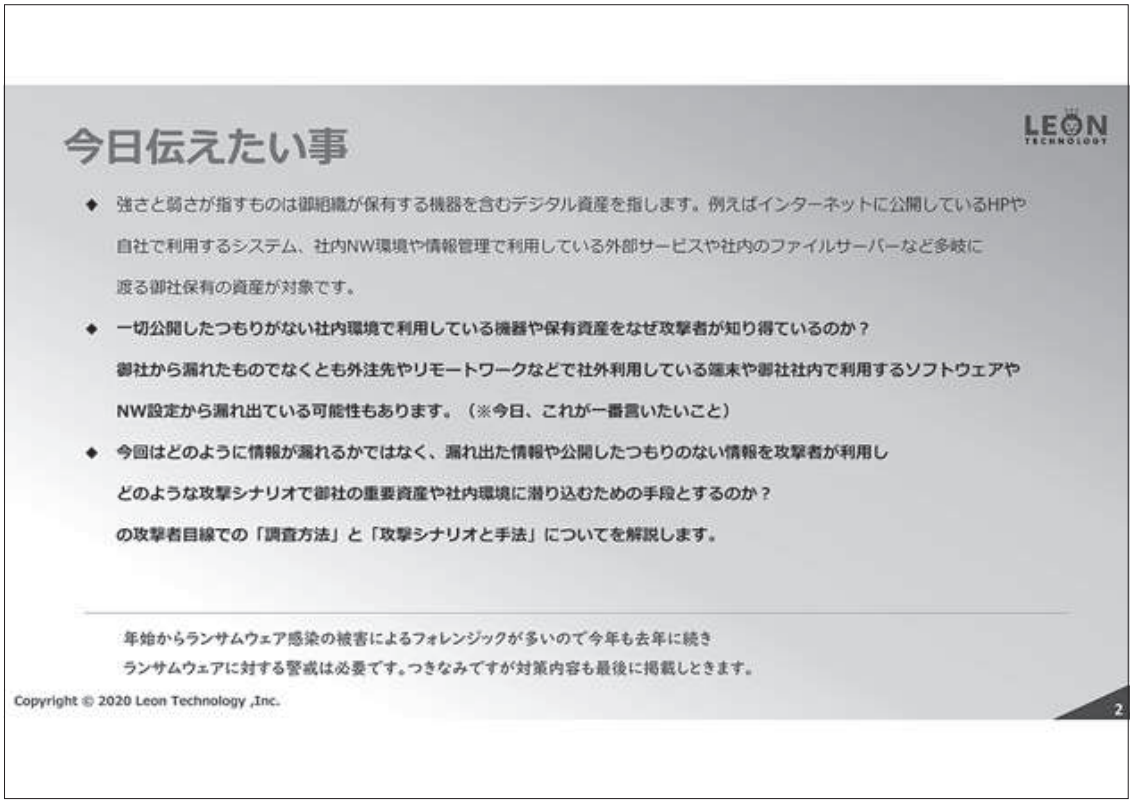
Slide 3　目次

「攻撃者は御社の強さと弱さをどう判断するのか?」。

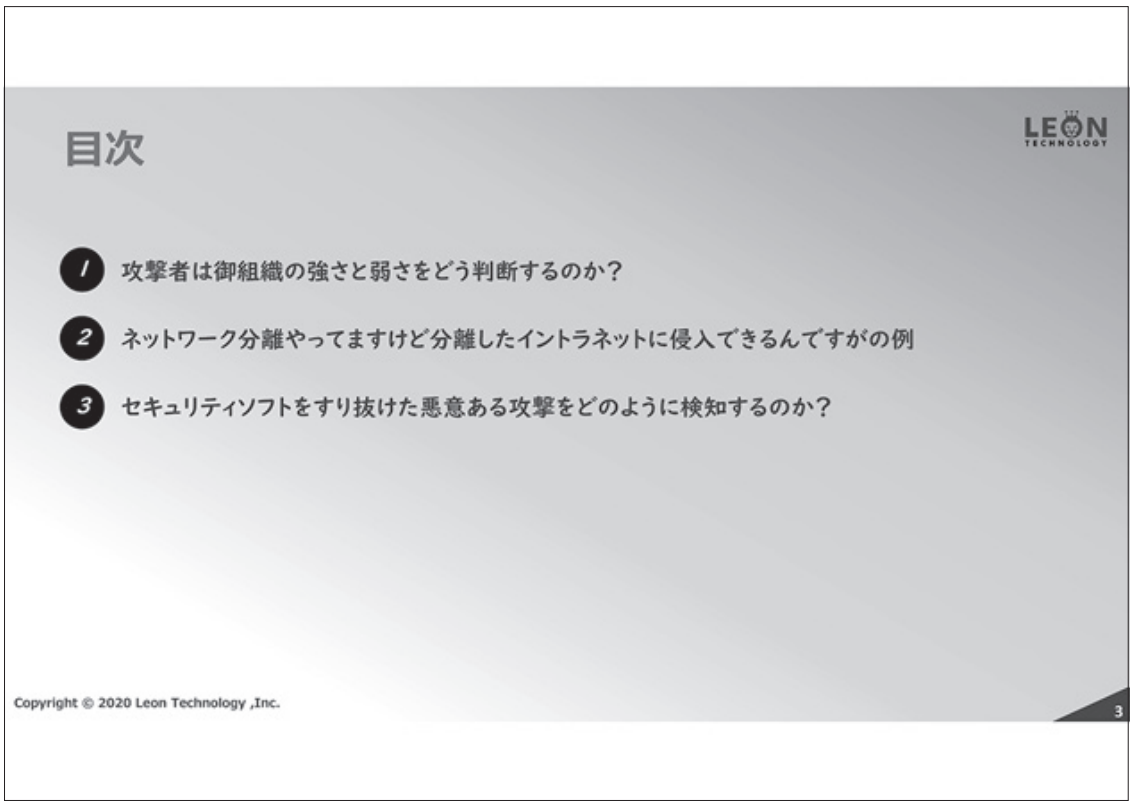
2 番目、「ネットワーク分離やってますけど、分離したイントラネットに侵入できるんですけど」っていう話ですね。

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?」というとこのお話です。

Slide 2



Slide 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けども、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ます。

ちょっと、次、いきますね。

Slide 4

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？

4

Slide 5

第一章　始める前の余談01

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/040947f596bd36b238367f2e77955a917fbca37e
https://japan.zdnet.com/article/35160009/

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こと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、既に情報が収集なされた 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にございますよと。

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 とかリモートワークとか、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 といわれるもん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使っている 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し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、「わなに引っかかった人」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顛末だったりとか、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の、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ある 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。