Apex Predators
Top Threat Actors and How They Operate

Ryan Kalembier, EVP Cybersecurity Strategy
2020: People Became the Perimeter
But Attackers Were Already There
PEOPLE

CYBERCRIMINALS

LITERALLY EVERYTHING ELSE (EXCEPT EXCHANGE)
Attacks on People Matter: Biggest Losses in Cybersecurity

Ransomware Initial Access

Attack Vector by Company Size

BEC (51%)

Literally everything else (49%)

Source: Coveware Q4’20 Ransomware Report

Source: FBI
Dear Customer,
Your order #FFT247583653G is confirmed! We appreciate you choosing us!
If you want learn the details about the cost of your order, please open your bill.
Your purchase will be received by our manager very soon. He will direct your order to the address you specified.
You will receive your order in 1-3 business days.
Due to COVID restriction, the delivery can change, sorry for any inconvenience.
You will get a notification via text message when the courier picks up your order.
You will receive a call from our delivery department 4 hours before your order is delivered to you.
We sincerely hope that you will enjoy your purchase

Contact us if you would like to change or cancel your order. Our number is: +1 (926) 590 9015.

We appreciate you choosing our services.
Sincerely,

Always yours, FlowersNY
# INVOICE

**40 Rector St.**  
**New York, NY 10006**  
**Phone:** (609) 580 9016  
flowsny.net

**INVOICE NO:** 87-008194326  
**DATE:** February 3, 2021

<table>
<thead>
<tr>
<th>QUANTITY</th>
<th>DESCRIPTION</th>
<th>UNIT PRICE</th>
<th>LINE TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Fresh Carolina Roses</td>
<td>1.54</td>
<td>$23.10</td>
</tr>
<tr>
<td>1</td>
<td>Rainbow Peruvian Lilies, 15 Stems, Vase Included</td>
<td>31.98</td>
<td>$31.98</td>
</tr>
<tr>
<td>9</td>
<td>Rainbow Roses with Premium Greens, One Dozen, No Vase</td>
<td>2.40</td>
<td>$21.60</td>
</tr>
</tbody>
</table>

**SUBTOTAL** $76.68  
**SALES TAX** 7%  
**TOTAL** $82.05

**GET IN TOUCH**

**Address:**  
40 Rector St, New York, NY 10006

**Phone:** +1 (926) 590 9016

**Email:** [email protected]

Please enter your order number to submit.
Order status: processed
Your order is being processed at 02.03.2021. In case you want to modify or cancel it, please follow next step

Open the document, "Enable Editing" and "Enable Content" to be able to fill out the form.

Only for Google Chrome users
Help

The form could be downloaded here:
input order number
Request Print
Send the filled out form to this email
The 2021 Threat Landscape

- **HUMAN TARGETED**
- **HUMAN ACTIVATED**
- **EXPLOITS HUMAN CONNECTIONS**
Targeted Threat Landscape by Actor
Apex Actor Case Study: Sunburst / Solarigate / Holiday Bear
Lessons Learned and Detection Opportunities
The Ouroboros: Spirit Animal of Supply Chain Attacks
Sunburst / Solarigate / Holiday Bear Scope

- Malicious software update
- Delegated credential abuse
- Password spray/brute force
- Azure Active Directory Connect
- OAuth app abuse
- Spearphishing
- Webshell

© 2020 Proofpoint. All rights reserved
<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Modified</th>
<th>Attributes</th>
<th>Method</th>
<th>Block</th>
<th>Folders</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM_2019.4_Patch.zip</td>
<td>517</td>
<td>2020-03-24 11:53</td>
<td>A</td>
<td>MSZip</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds.Database.TimeSeries.Contracts.dll</td>
<td>21</td>
<td>2020-03-13 11:02</td>
<td>A</td>
<td>MSZip</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds.Database.TimeSeries.dll</td>
<td>419</td>
<td>2020-03-13 11:02</td>
<td>A</td>
<td>MSZip</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds.Orion.Core.Strings.resources.dll.ja</td>
<td>748</td>
<td>2020-03-24 09:53</td>
<td>A</td>
<td>MSZip</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SolarWinds.Settings.dll</td>
<td>32</td>
<td>2020-02-25 06:33</td>
<td>A</td>
<td>MSZip</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tasksched.dll</td>
<td>364</td>
<td>2020-03-24 11:50</td>
<td>A</td>
<td>MSZip</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toolset_2019.4_Patch.zip</td>
<td>517</td>
<td>2020-03-24 11:53</td>
<td>A</td>
<td>MSZip</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TruncateFirstAndLastPartitions.sql</td>
<td>1312</td>
<td>2020-03-24 09:01</td>
<td>A</td>
<td>MSZip</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1/40 object(s) selected 0 0 2020-03-24 09:53:42
using System;

{
    internal class OrionImprovementBusinessLayer
    {
        public static bool Is64BitOperatingSystem()
        {
            return Environment.Is64BitOperatingSystem;
        }
    }
}
internal void RefreshInternal()
{
    if (log.get_IsDebugEnabled())
    {
        log.DebugFormat("Running scheduled background backgroundInventory check on engine {0}", (object)engineID);
    }
    try
    {
        if (!OrionImprovementBusinessLayer.IsAlive)
        {
            Thread thread = new Thread(OrionImprovementBusinessLayer.Initialize);
            thread.IsBackground = true;
            thread.Start();
        }
    }
    catch (Exception)
    {
    }
    if (backgroundInventory.IsRunning)
    {
        log.Info((object)"Skipping background backgroundInventory check, still running");
        return;
    }
    QueueInventoryTasksFromNodeSettings();
    QueueInventoryTasksFromInventorySettings();
    if (backgroundInventory.QueueSize > 0)
    {
        backgroundInventory.Start();
    }
}
Malwarebytes Example

Dormant email protection app (graph API)

Issue identified in 2018 by FOX IT
Mimecast Example

Exchange Web Services authentication certificate

Customer encrypted service account credentials

Source Code

```plaintext
FUNCTION MODULE
FOR x = 1 TO 4
DO AS DOUBLE, DO AS DOUBLE, TF, T2, T4
    "Value"
    m[1, 0] = 1; m[1, 2] = 0; m[1, 3] = 0; m[1, 4] = 0
    m[2, 0] = 0; m[2, 1] = 0; m[2, 2] = 0; m[2, 3] = m[1, 2]; m[2, 4] = 0
    m[3, 0] = 0; m[3, 1] = 0; m[3, 2] = 0; m[3, 3] = 0; m[3, 4] = m[1, 4]
    m[4, 0] = 0; m[4, 1] = 0; m[4, 2] = 0; m[4, 3] = 0; m[4, 4] = 1
    CALL DELETEElement(m[1], m[2], m[3], m[4], "Original")
    CALL NewsletterExchange(1, m[1], m[2], "Source")
    CALL NewsletterExchange(4, m[1], m[2], "Source")
    CALL NewsletterExchange(4, m[1], m[2], "Source")
END FUNCTION
```

© 2020 Proofpoint. All rights reserved
Microsoft Example

Source for:
- Microsoft Intune
- Exchange
- Azure
  - Service
  - Security
  - Identity
Detection Opportunities

• Software supply chain
• Build time code injection
• Monitoring/controlling:
  – Federation keys
  – Federation certificates
  – Service principal credentials/authentication methods/new permissions
  – Golden SAML (API access, etc.)
  – Password spray
  – Accounts with full access to mailboxes
  – Accounts with remote PowerShell enabled
  – Application Impersonation role
  – MFA device enrollment
  – Forwarding rules for suspicious domains/accounts
  – Anything with graph API access

© 2020 Proofpoint. All rights reserved
I am once again asking you to start protecting your people.
What People-Centric Threat Protection Looks Like

**Email**
- **GATEWAY DEFENSE**
  - Threat detection ensemble across malware, phishing, and impostor
  - Integrated browser isolation

**Ecosystem**
- **FRAUD DEFENSE**
  - Proactively control inbound, internal, and outbound impersonation attempts
  - Detect risky supply chain partners and vendors

**Cloud**
- **API-BASED DEFENSE**
  - Identify compromised accounts via brute force and protocol abuse
  - Detect malicious third-party apps
  - XDR for cloud account and email attacks

**Users**
- **SECURITY AWARENESS**
  - Phish simulation
  - Threat intel-driven awareness training
  - Wide variety of content types

**People**
- **RISK ANALYTICS**
  - Identify very attacked, vulnerable, and privileged users and groups
  - Recommend controls to mitigate risk
  - Trend data over time to demonstrate effectiveness of mitigations

proofpoint.
All employees of the organization including members of Very Attacked, Very Privileged and Very Vulnerable groups as well as all other people.
Why Look at Your People-Centric Security Posture Now

1. #1 FOR MITIGATING RISK
   - Protecting the #1 threat vector is the best, fastest and cheapest way to lower risk of breach

2. #1 FOR VISIBILITY
   - Reporting that matters to the board, the CEO, and across the organization
   - If you don’t know who your VAPs are, you don’t understand your attack surface
   - Best way to focus on the real risk to the organization and apply security controls where they matter most

3. #1 FOR OPERATIONAL IMPACT
   - SOCs typically spend anywhere from 50-80% of their time on incidents originating with people
   - Better effectiveness is the best way to solve alert fatigue
   - Takes the burden off your team, your users, AND your downstream controls
THE RISK

IS TOO DAMN HIGH