TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Don’t Get Phished

in the Rising Tide of

Phishing

Phishing is one of the escalating and hard-to-detect threats for all Internet users as it does not seem malicious at first look. Over the last few months, it's frequency and intensity has increased significantly. Researchers from Barracuda Networks reported that COVID-19 related phishing attacks have increased by 667% since the end of February 2020. The cybercriminals are leveraging the amplified focus on COVID-19 to deliver malware and scam victims out of money. They are also using the renowned brands to trick people and steal sensitive information like personal data and login credentials. As per the Q1 2020 Phishing Report from Check Point - Apple, Netflix, Yahoo, WhatsApp & PayPal are the top 5 mimicked brands for phishing attempts.

This tremendous growth in phishing attempts is posing a great challenge for organizations as a majority of businesses are running remotely. Thus, organizations must understand different phishing techniques and thereafter make employees aware of them through proper security awareness training.

Different Phishing Techniques

Deceptive Phishing

This is the most common phishing attack in which attackers impersonate a legitimate organization to make victims believe that the received email is originated from an authentic source. Such emails come with a sense of urgency i.e. requesting users for immediate actions like log-in to change passwords, payment failure, etc.

Spear Phishing

It is an in-depth version of deceptive phishing that incorporates specialized information about the victim. For instance, it might include information of employees within an organization or personal details of the targeted entity. This helps threat actors to make victims believe that they have a connection with the sender. Social media websites are common sources for attackers to get relevant information about the target.

Clone Phishing

In such phishing attacks, cybercriminals create an identical copy or clone of the legitimate, previously transferred email messages and then replace the attachment with a malicious file or link it to an infected URL. When the victim receives the infected email, it appears to come from the original sender. Therefore, it is much harder to detect than other common phishing attacks.

Whaling

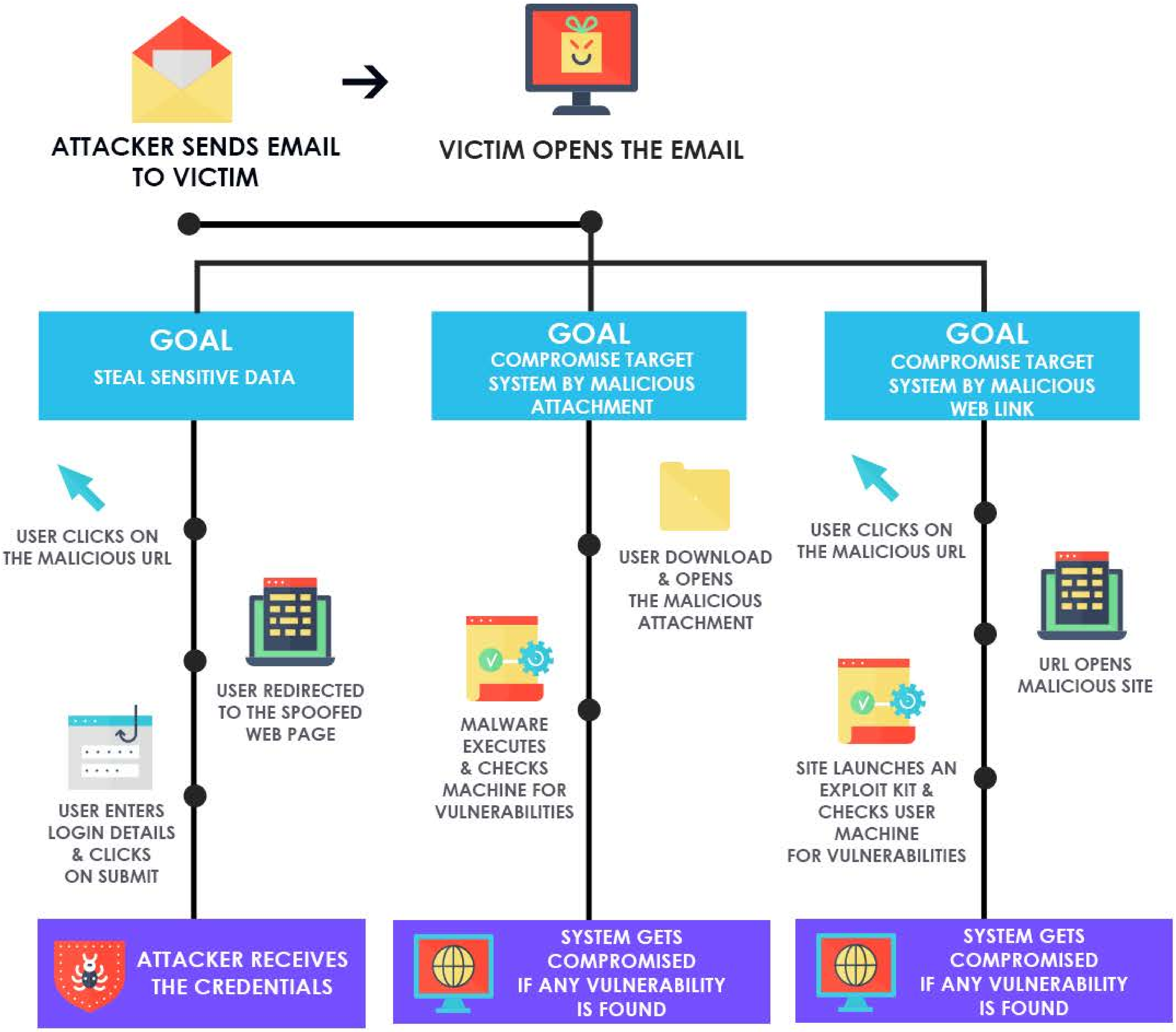
This type of phishing attack is directed to target high-profile, senior-level executives of an organization with the aim of stealing money, sensitive information or gaining access to their computer systems. Cybercriminals masquerade themselves as a senior employee like Finance Manager or Board Member and send malicious emails containing relevant information gathered online to the target employees.

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

How Victim Gets Infected



ATTACKER SENDS EMAIL TO VICTIM → VICTIM OPENS THE EMAIL

GOAL
STEAL SENSITIVE DATA

- USER CLICKS ON THE MALICIOUS URL
- USER REDIRECTED TO THE SPOOFED WEB PAGE
- USER ENTERS LOGIN DETAILS & CLICKS ON SUBMIT

ATTACKER RECEIVES THE CREDENTIALS

GOAL
COMPROMISE TARGET SYSTEM BY MALICIOUS ATTACHMENT

- USER DOWNLOAD & OPENS THE MALICIOUS ATTACHMENT
- MALWARE EXECUTES & CHECKS MACHINE FOR VULNERABILITIES

SYSTEM GETS COMPROMISED IF ANY VULNERABILITY IS FOUND

GOAL
COMPROMISE TARGET SYSTEM BY MALICIOUS WEB LINK

- USER CLICKS ON THE MALICIOUS URL
- URL OPENS MALICIOUS SITE
- SITE LAUNCHES AN EXPLOIT KIT & CHECKS USER MACHINE FOR VULNERABILITIES

SYSTEM GETS COMPROMISED IF ANY VULNERABILITY IS FOUND

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Data Compromised During A Phishing Attack

Personal Identifiable Information like complete names, residential addresses, birthdates, social security numbers etc. The attackers could use such data for identity theft.

Financial Information like credit/debit card numbers, bank account numbers, etc. Hackers can utilize this data to steal money and commit fraud.

Company Information like ongoing projects, partner & client information, sales database, etc.

Contact Numbers help cybercriminals to bypass the two-factor authentication as well as launch smishing campaigns.

Usernames and Passwords let attackers to login into your personal and corporate accounts and cause severe damage.

TATA

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

How To Deal With Phishing

Recommended security controls for organizations to combat with the increasing phishing attacks:

- Implement two-factor authentication (MFA) as it adds an additional layer of security while logging into critical applications or resources.
- Use email filters to highlight high-risk email messages.
- Implement Anti-Phishing or complete Email Security solutions to prevent phishing emails from reaching the inboxes of your employees.
- Use a robust web application firewall to block malicious requests.
- Conduct security awareness programs to keep employees aware of the possible threats.

Recommended security practices for employees to avoid falling prey to attackers:

- Never click on links or download attachments from unknown or unauthorized sources.
- Never send critical information like credit/debit cards pin or internet banking credentials over email or text.
- Always look for red flags like generic greetings, spelling and grammatical errors, urgent action requests, wrong logo, etc in the suspicious emails.

The Cyber Security Practice of Tata Advanced Systems is constantly supporting businesses to transform their cyber defence and continue operations in a secured environment through its comprehensive cybersecurity services.

To know more about our offerings, reach us at

contactcs@tataadvancedsystems.com