nccgroup
freedom from doubt

An NCC Group Publication

Modelling Threat Actor Phishing Behaviour - “you're only as strong as your weakest link!”

Prepared by:

E D Williams

ed.williams ‘at’ nccgroup ‘dot’ trust

Contents

Document History

Issue No.	Issue Date	Change Description
1.0	22/07/2015	Approved for public release

1 Introduction

NCC Group is a leading provider of professional red teaming, phishing and other forms of real-world attack simulation. Our extensive cyber incident and defence operations experience has resulted in us gaining significant insight into the techniques and methodologies used to breach organisations of all types.

More and more organisations use simulated attacks of varying levels to more closely and accurately model threat actor behaviour, in order to measure their end-to-end resilience. The outputs from these activities are then used to measure and improve their defences, be they technology, process, or people, by incorporating the lessons learnt. One element of these simulated attacks often used is phishing, due to its prevalent use by nearly all threat actor groups.

This whitepaper will discuss how likely targets are identified and why certain individuals become targets. It will also cover why the timing of attacks affects the likelihood of success. Finally, resiliency strategies for both organisations and users will be suggested, to assist in reducing the likelihood and success of an organisation and individuals being targeted.

1.1 What is a simulated attack?

A simulated attack attempts to mimic a real-world attack by modelling the threat actors and their techniques. It is important to remember that a simulated attack is designed not to disrupt any business services or processes, like most threat actors.

This whitepaper will mainly focus on the reconnaissance phase of the simulated attack. The reconnaissance phase will typically involve open-source intelligence (OSINT), cyber intelligence (CYBINT), and human intelligence (HUMINT), in which the target organisation and potential individual targets are identified.

2 Why certain individuals or roles are good targets

Careful consideration is given when selecting individuals for targets; the success of the whole campaign can rest on these individuals, so careful and subtle discovery and profiling is required. Certain categories of individuals and specific functional roles are, in NCC Group's experience, far more attractive to a threat actor as they, in the main, yield greater success.

While there are no hard and fast rules for individual and role selection, some high-level guidelines are given below.

2.1 Individuals and roles resulting in higher likelihood of success

The following table highlights the types of individuals and roles that are often targeted and the typical reasoning:

Individual/Job Role	Reasoning
Non-technical[1]	A non-technical team member is, from our experience, more likely to click on malicious links or open malicious documents than a technical user.
Human Resources (HR) Staff	HR staff often deal with electronic documents from untrusted sources as part of their role. This fact results in a far greater success rate when using malicious CVs and similar to launch attacks.

[1] There may be good reasons to attack technical users; for example, they have privileged access to systems or environments. If this is the case, care should be taken, and the individual should be thoroughly profiled through the reconnaissance OSINT phase, and all communications highly tailored.

Individual/Job Role	Reasoning
Internal Recruitment	Like HR staff, internal recruiters are more likely to open electronic documents, such as CVs, from untrusted sources.
Accounts Payable	Accounts payable staff will likely receive and send emails from clients; as such they would be an interesting target. Note that this team may have the facility to transfer funds so are often a target for criminals.
PR, Marketing and Social Media Teams	These teams are used to interacting with external parties, transferring documents and other attachments, visiting links, and similar. This group also typically has access to an organisation's social media platform which can be a target for groups seeking to repurpose it for propaganda.
Executives	Through spear-phishing, executives can be enticed to open malicious documents that may, for example, contain a C-level job advertisement and other similar flattering communication.
Receptionists/Personal Assistants (PAs)	Administrative personnel are, by their very nature, helpful, and are more often than not conscientious; this desire to help can be exploited with a phishing attack.
Sales Team	Members of the sales team are viable targets as they quite often have sales targets and thus are driven, with a "close down every opportunity" attitude, which can be exploited by sending a malicious e-mail or document with a specific sales slant to it.
Customer Service Team	Members of the customer service team, depending on the business, may be used to interacting with documents and links from untrusted sources.
Have been involved in a previous breach	During the OSINT phase, previous breach information will be examined. If a user is found, this information could be used in a phishing campaign.
Heavy social media user	Heavy social media users will inevitably disclose personal information; the more information that can be gathered, the greater the degree of analysis that can be performed about the individual. With greater information, a successful targeted attack is more likely.

2.2 Individuals and roles resulting in lower likelihood of success

While some individuals can increase the likelihood of success, the converse of this is also true: some individuals and roles are less likely to yield results, and could even nullify the campaign by alerting the blue team, helpdesk, or security staff. As such, careful consideration should be given to these individuals even if their perceived access makes them may appear to be interesting targets.

The following table highlights individuals or roles that are not considered viable targets in the first wave and should be avoided unless there is specific OSINT from the reconnaissance phase which indicates otherwise:

Individual/Job Role	Reasoning
Technical users	A technical user is likely to detect an attack and alert the blue team or protective monitoring.
Cyber-security staff	Security staff members are likely to identify a phishing attack; however, this could be a source of major embarrassment if they are targeted and successfully phished.
Cyber-security hobbyists	Along with traditional information security staff, information security hobbyists should be avoided. This information can be determined during the OSINT/CYBINT phase of the campaign.

However, although they are more savvy, technical teams should not always be discounted, as anyone in an organisation can become overconfident or otherwise be busy, and click on links or open attachments that would represent a risk.

3 How individuals and roles are discovered

Discovering individuals and roles is a critical step within the OSINT reconnaissance phase. It can be normal for the OSINT phase of a project to be the longest phase, and to yield few up-front results; however, ultimate success comes from a detailed and thorough discovery and profiling of potential targets. There are many, many sources that can be used to gather OSINT; the following list is given as an example of typical starting points.

3.1 Company director records/company profiles/about us etc.

Enumerating the target organisation, and subsequently individuals, is the first stage during the reconnaissance phase. Company records, from Companies House for UK organisations, for example, can be examined and analysed for financial intelligence (FININT). social media (see section 3.2), organisation web-site and more generic Internet searches, and technical sources such as DNS and IP WHOIS information, can reveal and profile target organisations.

3.2 Social media

Social media can be a treasure trove of information; individuals will often post sensitive information on social media that can be used to gain further insight into the target. Such information could be used for a targeted spear-phishing attack or campaign.

The following table highlights some of the most popular social media sites. Depending on the organisation or individual that is being targeted a wider search and analysis is often required; however, the following will act as a starting point:

Social Media Site	Available Information
Facebook[2]	Social media site, users post information from their personal life; this can include birthdays, political views, if they are on holiday, where they are, and what they are doing.
Twitter[3]	A micro-blogging site, location information can be enumerated, along with personal and work-related information, to tailor phishing emails.
LinkedIn[4]	A professional social media network, useful for identifying where people work, job titles, and skills and connections.
Google Plus+[5]	Similar to Facebook, people post personal and work-related information.
FriendsReunited[6]	Friends Reunited is a portfolio of social networking websites based upon the themes of reunion, with research, dating, and job-hunting.

[2] https://www.facebook.com
[3] https://www.twitter.com
[4] https://www.linkedin.com
[5] https://plus.google.com
[6] https://www.friendsreunited.com/

192.com[7] and international equivalents	Publishers of an online directory of people and where they live from the electoral roll. This information is useful for creating personally-tailored emails.

Assuming consent, a common approach to gaining connections and information from certain sites such as LinkedIn is creating pseudonymous profiles and connecting to individuals through this mechanism; for example, many LinkedIn users will automatically connect to recruiters without hesitation. Doing this can introduce a threat actor to second-degree connections and beyond; having access to second-degree connections will allow a threat actor to profile more users, gain valuable information, and ultimately expand and enhance their reach during the OSINT/reconnaissance phase.

3.3 Previous security breaches

Sites like pastebin [8] and haveibeenpwned [9] can prove useful in identifying vulnerable targets. Usernames and passwords can be enumerated from previous security breaches and can be used in the following scenarios:

- Assuming client/target consent, use harvested credentials against social media sites to gain further information about the target;
- Used directly against target organisation infrastructure;
- Use this information to target individuals for a spear-phishing campaign.

3.4 Papers, blog posts, support forums, and Q&A sites

Organisations often also provide rich sources of information about their employees, their roles and their interests. In the following sections we touch on a few examples of such sources.

3.4.1 Papers

Whitepapers, such as this, can be examined from organisations and individuals to identify skills, areas, possible technology, and areas of interest that could then be used in turn to target individuals.

Whitepaper metadata can also be examined to enumerate information, including version information that can be used to leverage exploits.

3.4.2 Blog posts

Blog posts can give a useful insight into an individual's hobbies and interests, which in turn can be used to further tailor the targeting towards them; either by enumerating more information, or by directly targeting them through a spear phishing or watering-hole attack[10].

3.4.3 Support forums and Q&A sites

Q&A sites are popular amongst technologists for posing technology-related questions. They will often reveal in-house technology use, which can be useful if having to target a technical team and when more broadly targeting the organisation. Work-related email addresses are often used instead of generic addresses; this can also be useful in deducing the structure of such email addresses.

On Q&A sites, it is common for individuals to post questions; this information can be used to launch an attack, be it a watering-hole attack or spear phishing, disguised as an answer to their original question.

---

[7] http://www.192.com
[8] http://pastebin.com
[9] https://haveibeenpwned.com
[10] https://en.wikipedia.org/wiki/Watering_Hole

3.5 Recruitment websites

Recruitment websites can be useful in enumerating information from organisations; typical information that can be found includes technology used, skills required, and possible organisational contact information, which can be used to launch spear phishing attacks.

3.6 Conference speaker and attendee lists

Conferences and their attendee lists are an attractive proposition; conferences will often list speakers, a brief bio that can contain useful information, and possibly contact and social media information. Armed with this information, a flattering email could be crafted to entice the target to open a document or visit a domain under control of the attackers.

4 Common attack windows

The timing of an attack launch is an important consideration. Care should be taken when launching an attack, to ensure the highest likelihood of success.

The following table broadly outlines the types of attack and when best, in our experience, to launch scenarios and attacks:

Phishing Attack Pattern	When	Reasoning
Mobile cloud authentication reset credential phishing	Out of hours	Targets are more likely to check their mobile devices out of office hours, and thus such emails will appear more contextually accurate.
Outlook Web Access (OWA) credential phishing	Out of hours	Targets are more likely to use OWA out of office hours and will, depending on the organisation, often not have access to a security operations centre to report issues. This delay, should a phishing email be reported, increases the likelihood of success across a wider group.
Spear-phishing attack	N/A	Do not target too many users from the same department.
	Beginning of working day	Users are more likely to work through emails first thing in the morning.
	Lunchtime	Staff members are often more likely to read less-work-related email during their breaks; thus emails which target social-media-related activity, cat pictures, or similar are likely to succeed.
	Not on holiday	Ensure that users are not on holiday; these facts can be discovered during the reconnaissance phase.
	After a key organisational or personal event	Targeting with a topical email post-event, be it a conference, press release or seasonal event, often leads to success during spear-phishing campaigns.
Social media phishing	During office hours	OSINT will need to be used to determine when people are posting information on social media. They may have location services enabled, so a threat actor could determine their location; if this is during office hours then a platform could be determined along with specific phishing attack vectors.
	Out of hours	As above, typically, users will check social media on mobile devices out of office hours and so a specific platform could be determined along with specific phishing attack vectors.

5 Resiliency strategies for organisations and users

The following recommended high-level strategies and recommendations should be used to make an organisation and its employees more resilience against the techniques outlined in this paper. While there is no single silver bullet to entirely remove the likelihood, success, and impact of an attack, a holistic defence-in-depth approach is recommended, to minimise the risks where possible.

5.1 User awareness and training

Continual awareness and training is an important part of any strategy for minimising the likelihood of successful attack, and for early reporting of any attempts. The ISO 27001[11] framework incorporates user awareness and training controls. Users should receive cyber-security training, including phishing, when they start and then at regular intervals as a top-up. Specifically, they should be made aware of the information security policy and how it relates to them, and given general guidance around password selection, email best practice, risk of social engineering, common techniques, and social media etiquette.

5.2 Social media use guidelines

The following guidelines should be supplied to employees as suggestions to help secure social media use and thus minimise the risk of threat actors gaining valuable intelligence from such sites:

Where the word “appropriate” is used in the guidance, what is appropriate will depend on:

- Organisation type.
- Organisation sector.
- Role within the organisation.
- Other risk-carrying traits such as sensitive information or client access.

The high-level social security media guidelines are:

- List employer and role only if strictly required during employment.
- Configure social media security settings to an appropriate level.
- Enable strict privacy settings where appropriate.
- Disable location-based services by default when posting new content.
- Carefully consider connections to people.
- Use disposable or otherwise low-value passphrases to secure social media sites.
- Do not post sensitive information related to the organisation on social media sites.
- Report any suspicious new connection requests, friend requests, follower requests or similar.

It is important with such guidelines that the organisation provide clear messaging that the goal is to minimise risk to business, and not to impinge on or otherwise curtail personal activities. By doing so higher adoption and adherence to the guidelines is more likely.

5.3 Simulated phishing attacks to support training and effectiveness measurement

A trusted third party performing simulated attacks against your organisation will identify areas of weakness within a tightly controlled framework; users will be identified through OSINT and CYBINT, and with agreement they will be targeted. Outcomes from the simulated attack can then be fed into training and awareness of all internal users.

[11] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

5.4 Anti-phishing and malicious code technical countermeasures

An organisation's initial goal is often to stop initial attacks where possible. The technical countermeasures that exist today against phishing and malicious code range in sophistication, cost, and effectiveness.

Such technical countermeasures can consist of:

- Malicious code scanning.
- Email content or web link scanning.
- Web link virtualised/simulated/sandboxed processing and analysis for malicious behaviour.
- Clearly marking emails which originate from outside the organisation, to reduce the likelihood of spoofing.
- Attachment quarantining for those containing binaries or password protected.
- Virtualised/simulated/sandboxed attachment processing and analysis for malicious behaviour.
- Previously-unseen DNS domains added to a queue for investigation by the security operations centre.
- Email client 'report this email' button for supplying emails for investigation by the security operations centre.
- Desktop sandboxing around browsers and common programs used to open Internet-originating content.
- Application whitelisting.

These countermeasures, when combined, can provide a potent combination to reduce the likelihood that attacks will be successful.

5.5 Protective monitoring

Prevention strategies alone are not sufficient as part of a mature cyber-security strategy; it is also important to be able to detect incidents. A key element in being able to detect incidents is protective monitoring. Examples of protective monitoring include:

- Network-level signature-based threat detection.
- Network full packet captures, to facilitate investigation at key network choke points.
- Traffic pattern anomaly detection, ranging in sophistication from time and volume through to behaviour or protocol anomaly.
- End point activity logging[12] to facilitate investigations.
- Security function monitoring such as SIEM or broader protections.
- Key asset close protection monitoring.

In order to gain the maximum value from such protective monitoring it is critical that such functions be staffed appropriately. It is often the case that such functions are outsourced either in party or entirely to third parties such as NCC Group and 24/7/365 Security Operations Centres.

5.6 Overall cyber-security hygiene and resilience

While we have discussed a number of specific resilience strategy strands, overall cyber-security hygiene and resilience is also an imperative. From defence-in-depth concepts through to patching and credential management, all play a part in ensuring an organisation is resilient against attacks, be they successful or not.

[12] https://labs.nccgroup.com/windowsactivitylogger/

6 Conclusions

This whitepaper has discussed, at a high level, how simulated attacks can model threat actor behaviour, with specific emphasis on selecting individuals and roles as potential targets for phishing exercises.

When modelling threat actor behaviour, information is key; the more information that can be gathered, the greater the analysis that can be conducted and the more plausible, and ultimately more successful, an attack will be.

We have also outlined a number of key areas for organisations and individuals to consider when thinking about their resilience strategies. These areas include both technical and personnel-related capabilities.

Today a technology-focused set of countermeasures is not enough.

7 How NCC Group can help

NCC Group, as a global leader in the provision of cyber-security professional services and advice, can help organisations in a number of ways, including:

- Cyber strategy development and board level education.
- Phishing simulation
- Red teaming
- Protective monitoring and outsourced security operations centres
- Cyber incident response and defence operations

To arrange a follow-up, fill in the contact form located at https://www.nccgroup.trust/uk/contact-us/.

8 Further reading and references

8.1 Further reading

Cyber red-teaming business-critical systems while managing operational risk – https://www.nccgroup.trust/uk/our-research/cyber-red-teaming-business-critical-systems-while-managing-operational-risk/

Open Source Intelligence: the First Link in the APT Kill Chain – https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/february/open-source-intelligence-the-first-link-in-the-apt-kill-chain/

NCC Group now a CBEST Approved Penetration Testing Provider – https://www.nccgroup.trust/uk/about-us/newsroom-and-events/news/2015/february/ncc-group-now-a-cbest-approved-penetration-testing-provider/

Cyber Kill Chain – http://lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Local Administrator Password Solution (LAPS) – https://technet.microsoft.com/en-us/library/security/3062591.aspx

9 Acknowledgements

The author wishes to thank Will Alexander and Ollie Whitehouse of NCC Group for their peer review and valued suggestions.

