Thycotic Black Hat 2014 Hacker Survey Executive Report

Executive Summary

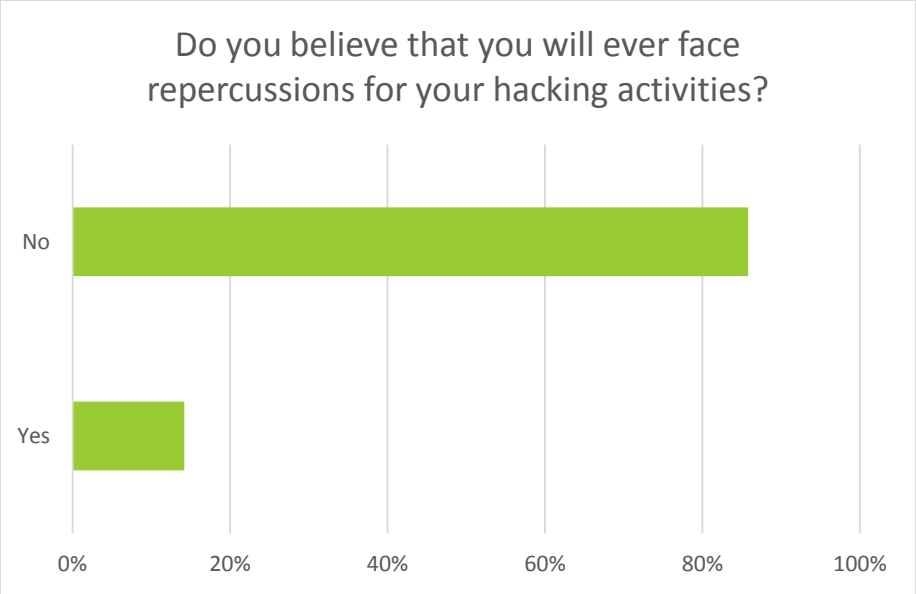
In a global marketplace dominated by information technology, hackers leverage various methodologies and have widely differing motivations for their illicit activities. As the headlines show, nation states and black hat technologists target global retail chains and government organizations for sensitive data that can be sold to the highest bidder. Other groups, such as hacktivists, are often veiled in anonymity and use their skills to bring social awareness to political issues through the manipulation of information technology.

In an effort to protect the integrity of their data security and reinforce trust among customers, organizations are taking heed of breach trends resulting in expanding IT security budgets. Not only is it important to understand how an attack was performed, but more importantly – why?

In order to develop an accurate psychological profile detailing the fears, expectations and motivations of today's hacker, Thycotic conducted a survey, live on site at BlackHat USA. Thycotic successfully secured 127 responses from self-identified hackers, despite the reluctance of this particular group to reveal details of their activities.

No fear: 86% of hackers don't believe they will be caught

An overwhelming majority of hackers surveyed don't believe they will face repercussions for their hacktivities. This indicates that without fear of accountability, there's increased motivation for continued hacking practices.



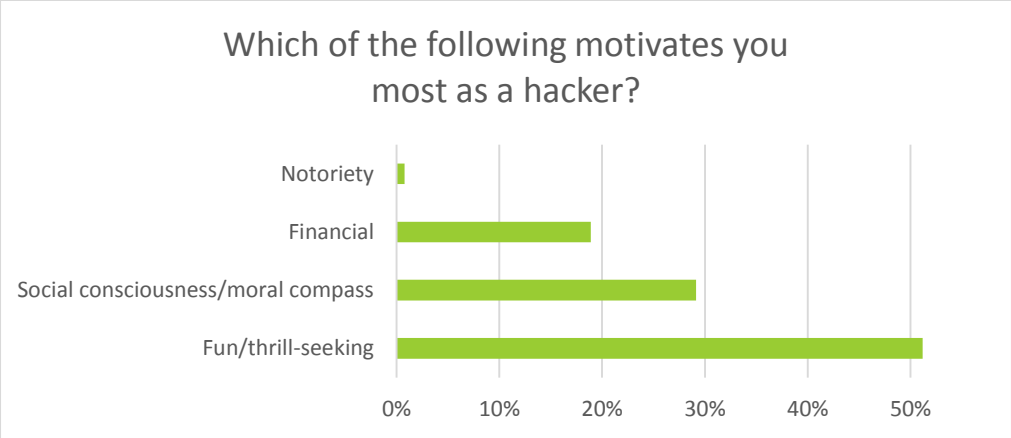
Why are hackers so sure they won't get caught? One theory is that the rate in which attacks are performed vastly outweigh how closely systems are monitored. Modern day hackers are more agile than ever, sporting a collective knowledge base of systems and programming languages at their disposal. This allows for bursts of attacks on multiple systems simultaneously, increasing success rates without adding much risk.

thycotic
IT Security That Works.
Thycotic Software Ltd
1101 17th Street NW, Suite 1102
Washington DC 20036
p: 1 202.802.9399
f: 1 202.315.3315
www.thycotic.com

Thycotic Black Hat 2014 Hacker Survey Executive Report

Hackers motivated by thrills, not dollars

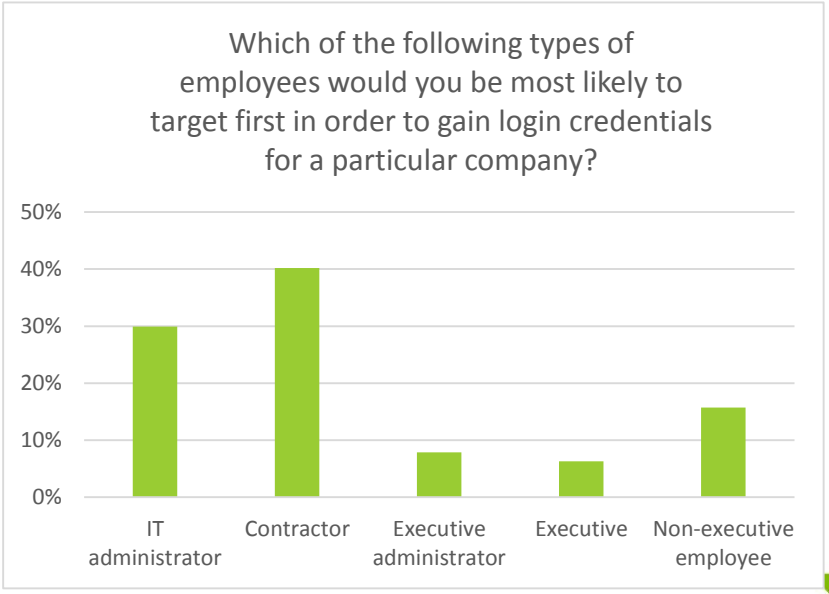
51% of hackers surveyed said that thrill-seeking motivated them in their activities, while only 18% noted financial gain as a direct motivation. What does this say about the modern hacker? Contrary to a majority of the news stories we read about ransomware and other forms of cyber blackmail, more than half of hackers who responded are simply curious, bored, or want to test out their abilities.



Primary attack targets: Contractors and IT administrators

40% of respondents said they would likely target contractors to gain login credentials.
30% of respondents placed IT administrators in a close second to contractors.
Only 6% would target executives for sensitive login credentials.

Both contractors and IT administrators are at a major risk for attack. These roles typically have direct access to servers and systems housing sensitive company data such as billing information and customer data. Once an attacker gains control of login credentials, they can swiftly compromise systems and gain control over the network. Intruders can scan systems for personally identifiable information, which is even more valuable to many hackers than credit card numbers or login credentials, because they can be sold on the black market and used repeatedly to create fake bank accounts or even file false tax returns.

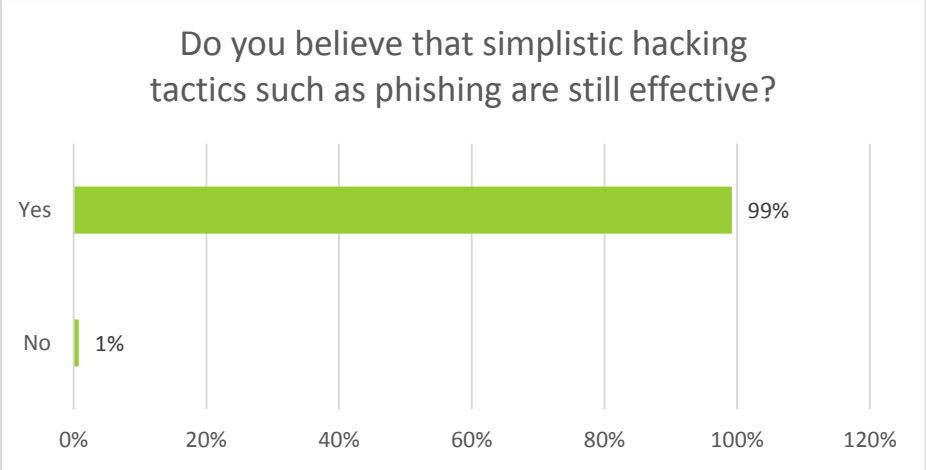


thycotic
IT Security That Works.
Thycotic Software Ltd
1101 17th Street NW, Suite 1102
Washington DC 20036
p: 1 202.802.9399
f: 1 202.315.3315
www.thycotic.com

Thycotic Black Hat 2014 Hacker Survey Executive Report

Stick with what you know: Phishing is still effective

More than 99% of respondents confirmed that "tried and true" methods of attack, such as phishing and spoofing, are still effective today. This means that the severity of an attack is not synonymous with complexity – and also, a hacker does not need sophisticated skills to succeed. Often, simple and effective tactics can be used to gain access to a variety of information.



Ultimate irony: Hackers fear their own information is at risk

A shocking 88% of respondents believe their own personally identifiable information is at risk for attack. If modern-day hackers are convinced they are at risk, what does this mean for the enterprise? Even the most talented of hackers are still susceptible to attacks, meaning data protection is more important now than it ever was.

thycotic
IT Security That Works.
Thycotic Software Ltd
1101 17th Street NW, Suite 1102
Washington DC 20036
p: 1 202.802.9399
f: 1 202.315.3315
www.thycotic.com

Thycotic Black Hat 2014 Hacker Survey Executive Report

Recommendations

As a necessary response for the upward trend in data breaches and global hacktivity, organizations are turning to effective privileged identity and access management, an arm of IT security that controls and monitors the privileges of highly sensitive systems and accounts. As the data shows, hackers are not hanging up their hats anytime soon.

Here are some best practices for organizations to help thwart a breach before it occurs.

1. **Strictly control privileged access.** Regarding primary hacking targets such as contractors and IT administrators, enforcing strict access to privileged accounts will help prevent a hacker from gaining login credentials on those systems. Set strict time frames on access to systems for contractors, immediately revoking access and changing system passwords after the contract has been fulfilled. For full-time IT staff, such as systems administrators, monitor and audit system usage on a daily basis. In the event that something was compromised, you can use the audit trail as a reference to investigate the event.
2. **Change system level passwords constantly.** For many hackers, the most valuable data is obtained by compromising system-level accounts such as servers, databases and service accounts. Make sure you're changing passwords on these accounts regularly, especially when working with contractors or if there is turnover in IT. This reduces the chance of an attacker obtaining those login credentials needed to cause further damage.
3. **Vault and restrict system-level credentials.** It's very important to understand how IT is currently managing the user names and passwords of systems on the network. Those utilizing poor practices, such as storing passwords in excel spreadsheets or worse – sticky notes tacked onto computer screens, are much more susceptible to losing their credentials to a malevolent outside force. Instead, make sure IT stores system level passwords in a vault (encrypted database on your network or for some organizations a physical vault). Here you can dole out access to systems as you need it and reduce the mindshare of passwords, which may thwart a phishing attack.

Survey Methodology

In August 2014, Thycotic surveyed 127 self-identified hackers live at the Black Hat 2014 event. "Hackers" were defined as official attendees of the Black Hat conference and personally identifying themselves as a hacker at the time of the poll. Respondents remained anonymous to protect their personal identity. For the complete survey, please email press@thycotic.com.

Thycotic Software Ltd
1101 17th Street NW, Suite 1102
Washington DC 20036
p: 1 202.802.9399
f: 1 202.315.3315
www.thycotic.com