



Welcome





LATIN AMERICA PRIVACY & CYBERSECURITY SYMPOSIUM

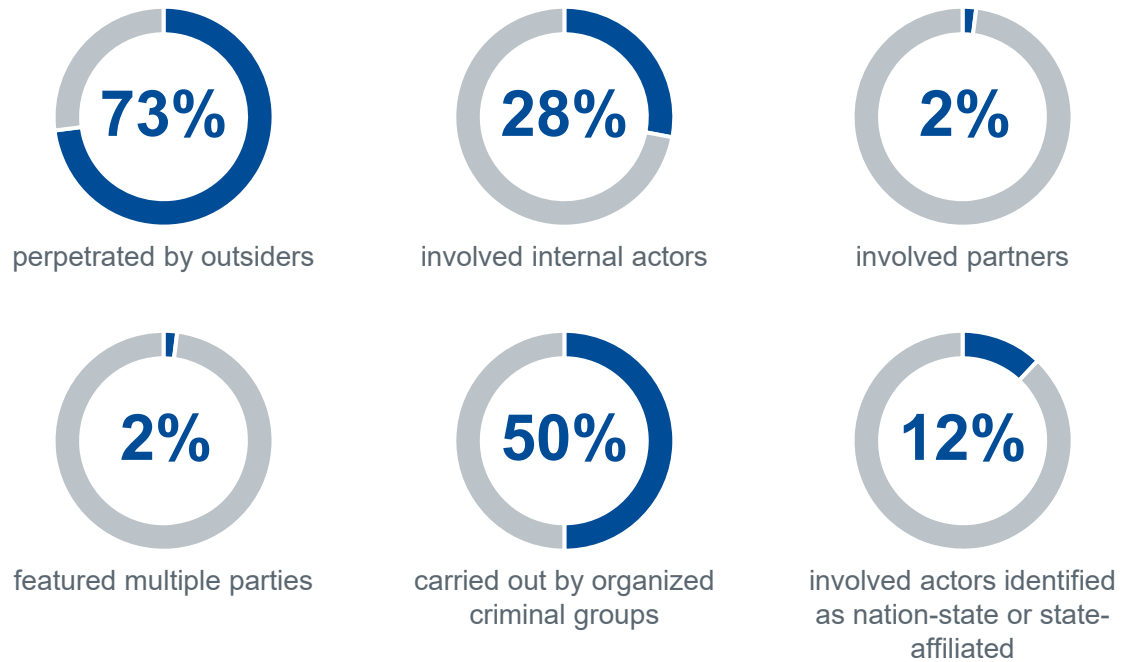
April 25, 2018

Presented by

The Crypsis Group
Sam Rubin








WHO'S BEHIND THE DATA BREACHES



Source: 2018 Verizon DBIR

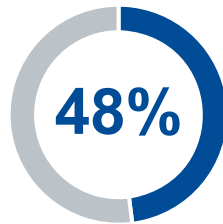


THREAT LANDSCAPE: WHO'S BEHIND THE BREACH?

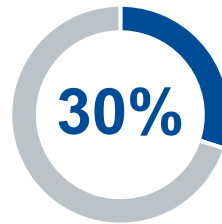
73% perpetrated by outsiders				28% involved internal actors
 <p>Cyber Criminals</p> <p>POTENTIAL IMPACTS</p> <ul style="list-style-type: none"> • Data theft <ul style="list-style-type: none"> • PII / PHI • Banking information • Cardholder data • Cyber extortion • Commodity malware • SPAM <p>MOTIVATION</p> <ul style="list-style-type: none"> • Financial gain 	 <p>Nation State</p> <p>POTENTIAL IMPACTS</p> <ul style="list-style-type: none"> • Loss of intellectual property • Destruction <p>MOTIVATION</p> <ul style="list-style-type: none"> • Cyber espionage • National security • Global competition 	 <p>Hacktivists</p> <p>POTENTIAL IMPACTS</p> <ul style="list-style-type: none"> • Data theft • Reputational damage <p>MOTIVATION</p> <ul style="list-style-type: none"> • Fame and glory • Ideological statements 	 <p>Cyber Terrorism</p> <p>POTENTIAL IMPACTS</p> <ul style="list-style-type: none"> • Mass destruction <p>MOTIVATION</p> <ul style="list-style-type: none"> • Political or national interest 	 <p>Insider</p> <p>POTENTIAL IMPACTS</p> <ul style="list-style-type: none"> • Data theft • Reputational damage <p>MOTIVATION</p> <ul style="list-style-type: none"> • Disgruntled employee • Financial gain



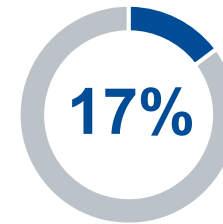
WHAT TACTICS DO ATTACKERS USE?



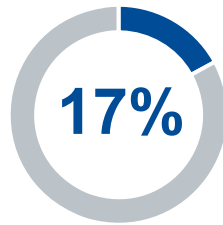
featured hacking



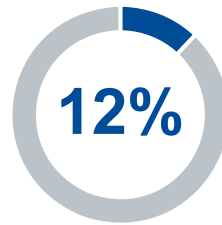
included malware



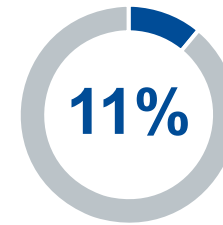
had errors as causal events



were social attacks



involved privilege misuse



involved physical actions

Source: 2018 Verizon DBIR



WHO ARE THE VICTIMS?

24%
of breaches
affected
healthcare
organizations

15%
of breaches
involved
accommodation
and food services

14%
were breaches
of public sector
entities

58%
of victims are
categorized as
small businesses

Source: 2018 Verizon DBIR



WHAT ELSE IS COMMON?

49%

of non-POS
malware was
installed via
malicious email

76%

of breaches
were financially
motivated

13%

of breaches were
motivated by the
gain of strategic
advantage
(espionage)

68%

of breaches took
months of longer
to discover

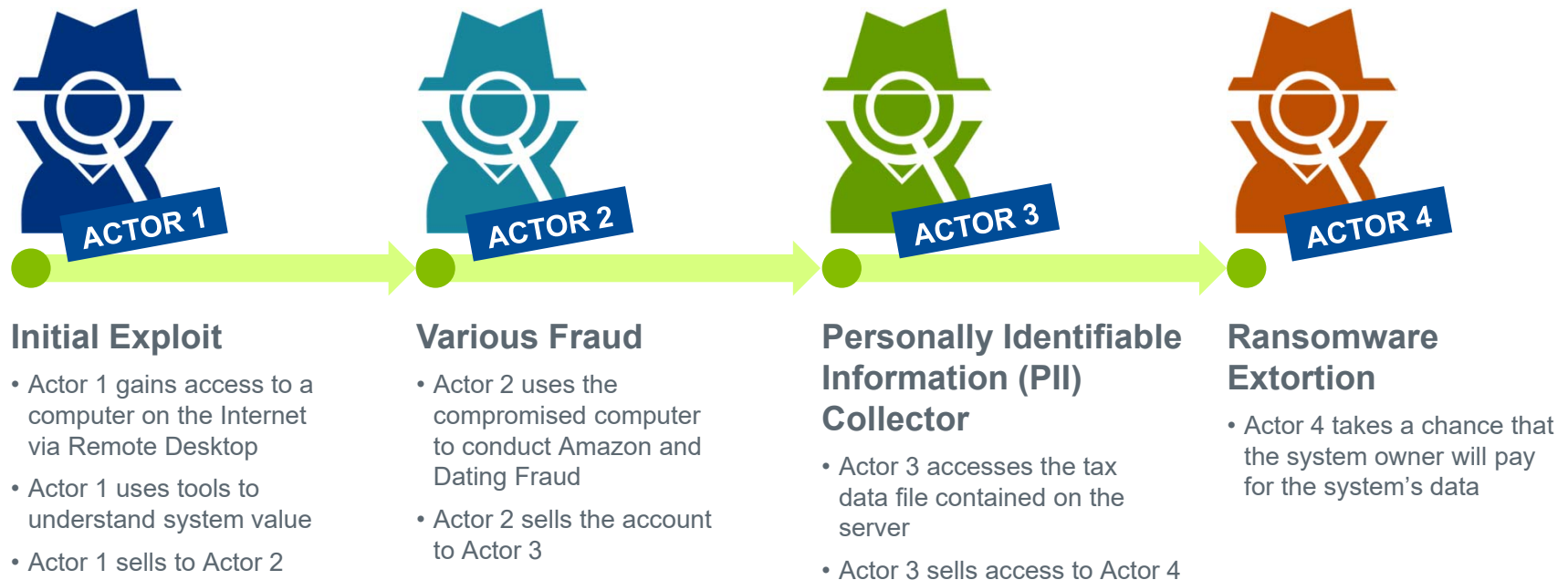
Source: 2018 Verizon DBIR



7



THE HACKER ECOSYSTEM



OTHER TRENDS



Strategic Operationalization

- Attacks pay off 3-9 months after date of initial compromise
- Credit Card attacks usually collect every 2-4 weeks and sell after 9-12 months



DarkNet Markets Sell Anything

- Credentials
- Personally Identifiable Information (PII)
- Proprietary Information



Ransomware Expansion

- Database extortions
- Email extortion



Creative Exploitation

- Customer lists exploited
- Public password dumps

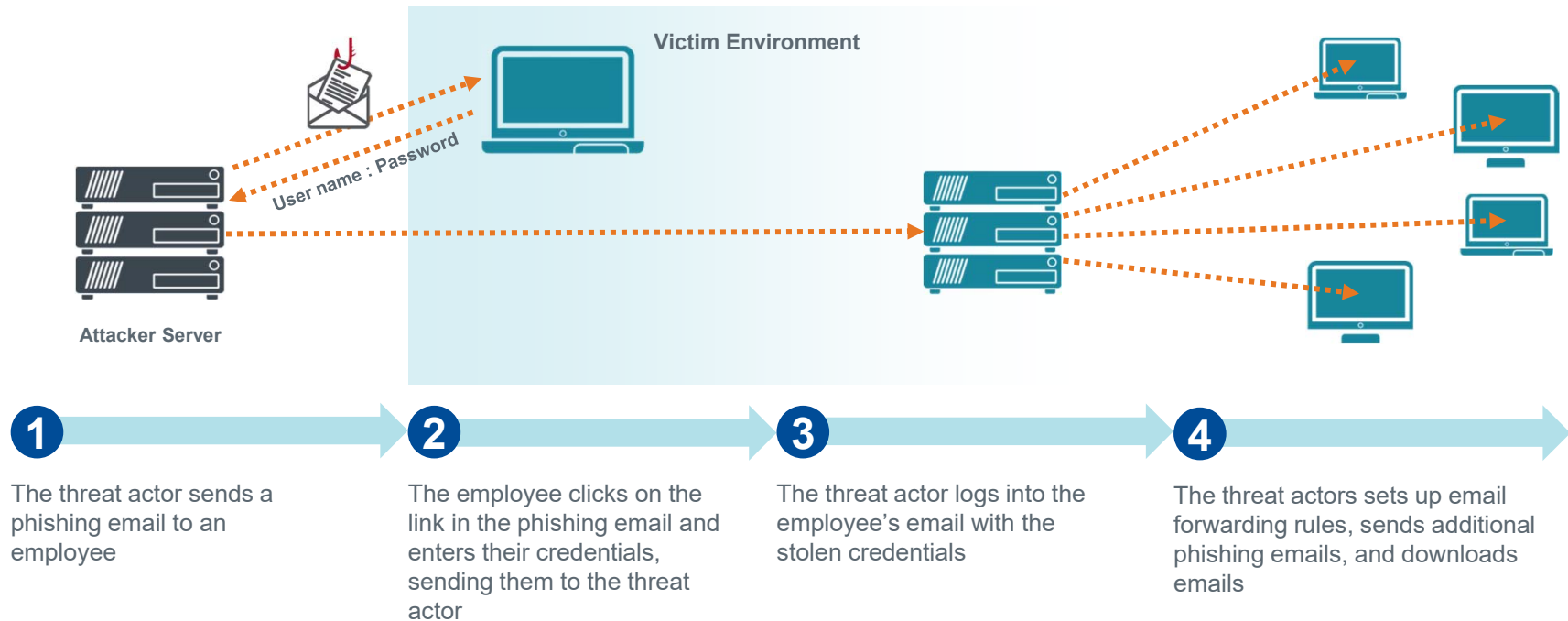


Phishing Attacks

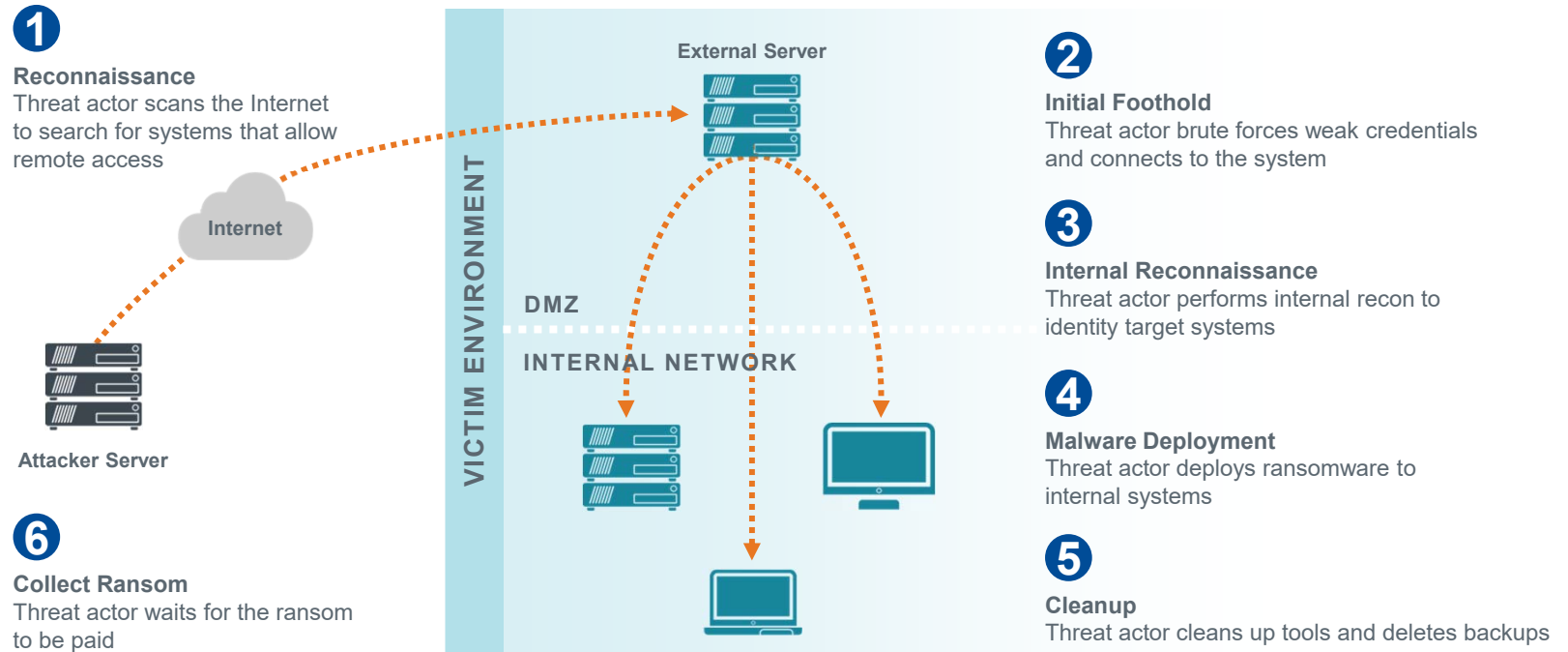
- Stealing employee information
- Stealing credentials



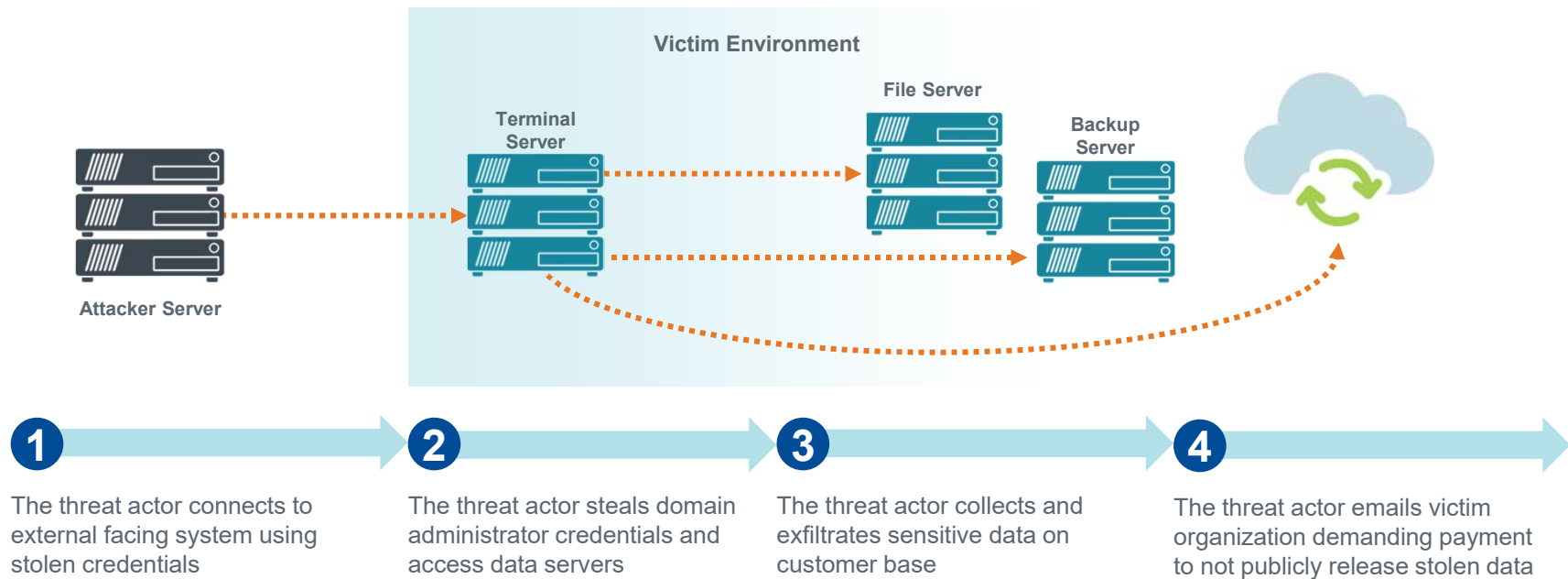
PHISHING EMAIL — UNAUTHORIZED ACCESS



ANATOMY OF THE ATTACK — RANSOMWARE



PUBLIC DATA RELEASE EXTORTION — ATTACK DETAILS



INCIDENT RESPONSE PROCESS



Designed for
agility and
efficiency



Speed: capable
of responding
within minutes



Collaborative
team approach



Proprietary
tools and
strategic
partnerships



Engaged by
outside counsel
through SOW on
99% of IR matters



Assist with
remediation
efforts during
the incident



crypsisgroup.com

