Stages of an Attack

Arrakis Consulting, LLC

Securing your world together

Company Overview

- Reliable
- Consistent
- Trusted Agent
- Proactive
- Forward thinking

Arrakis is uniquely positioned to provide numerous consultation and technology related services at all levels of business and all sizes or types of clients. Arrakis will help you to transform your IT operations from a reactive mode of crisis management to a proactive mode of preemptive management. We'll partner with you to determine your technology strengths and weaknesses, then quickly attack the weaknesses while minimizing any disruption to your business.

The leadership of Arrakis is composed of experienced business professionals with an extensive federal and military background. All members of Arrakis are required to conform to three key words of "Honor. Integrity. Excellence." and go through a rigorous validation process to ensure the highest level of professionalism.

Our experienced team of professionals have experience with commercial and government contracts of all sizes and price ranges and are available for remote or onsite support.

Contact Arrakis and lets secure your world together.

(Global average 28%)

What are the odds of an attack or a breach?

200+ days before detection

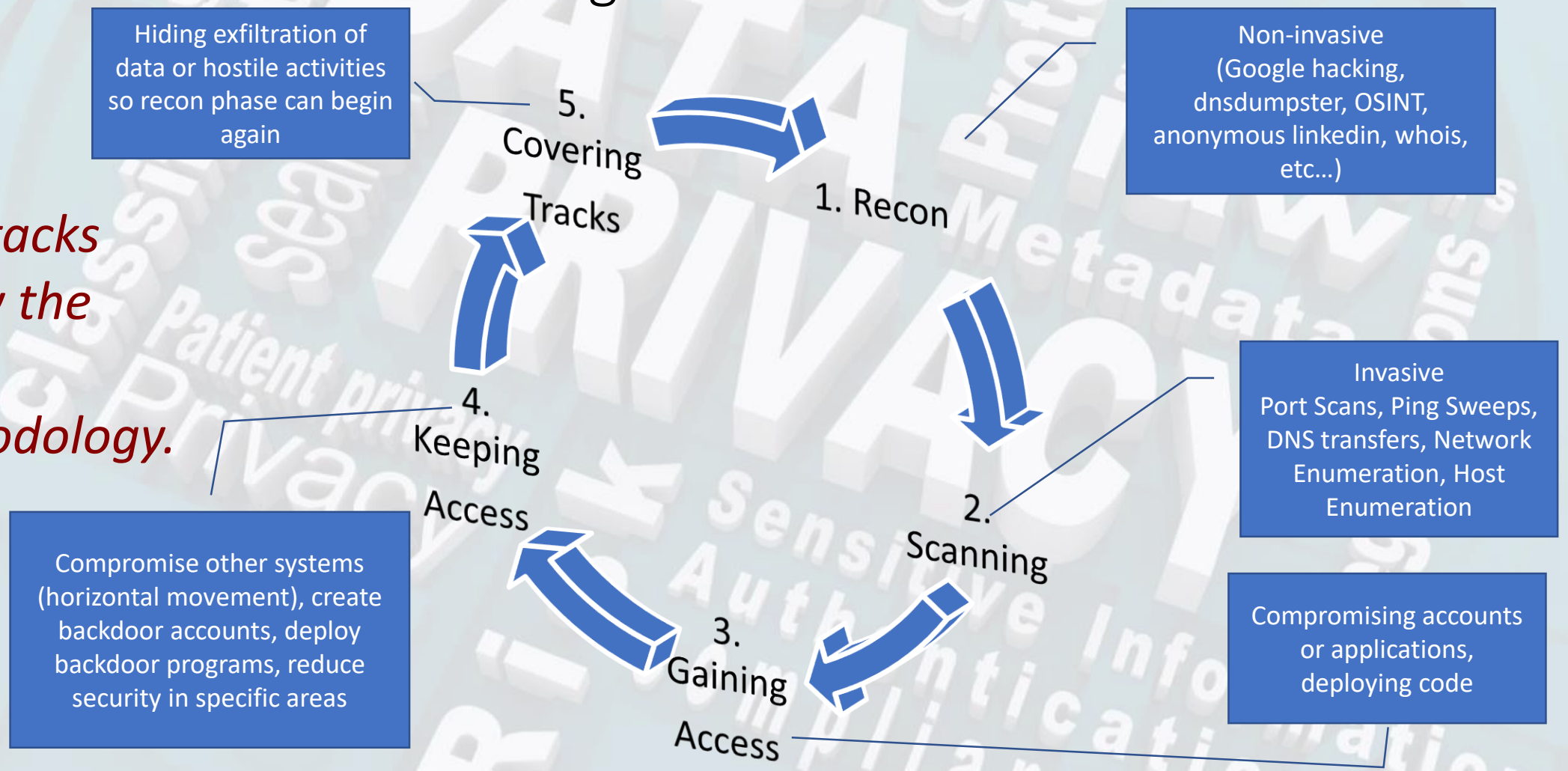
2016 update – "This year's study found the average consolidated total cost of a data breach is $4 million." *Ponemon Institute, 2016.*

75% due to compromised user accounts. This indicates a severe lack of awareness and security controls.

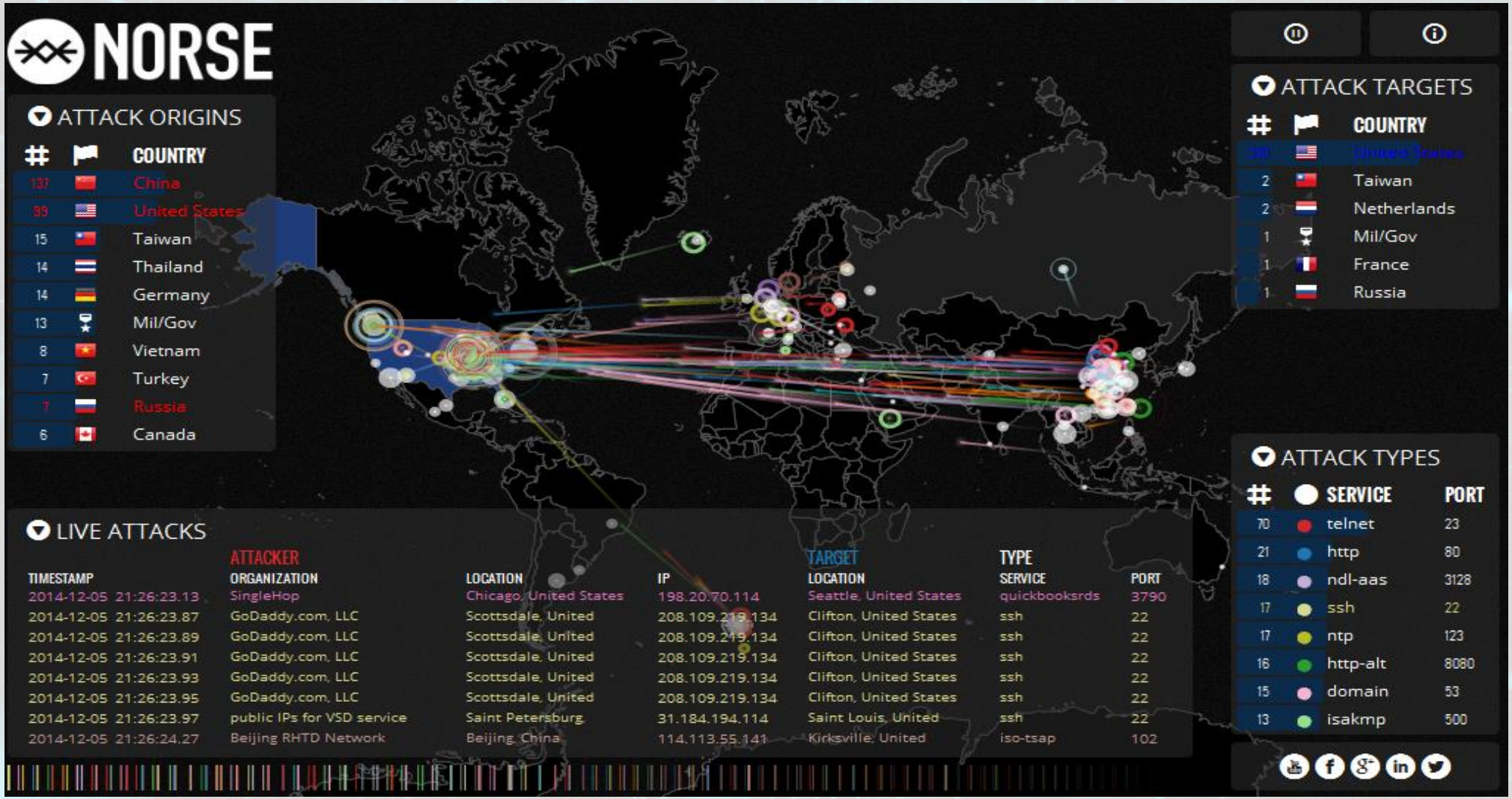
Update – "Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015." *Forbes, 2016*

What is the basic information?

Stages of an Attack



All attacks follow the same methodology.



View of an actual real time attack map.

Information Security

Ensure you are protected.

3rd Party Activities	• Arrakis can perform all aspects of acceptable 3rd party activities with special emphasis on vulnerability assessments, penetration testing, social engineering, physical security, and CISO as a service.
Investigations	• An investigation performed without a complete understanding of how investigations should be performed will rapidly leave into failure. Arrakis has numerous years of experience in investigations of all types and understands the legal aspects of properly performing all activities.
Breach Remediation	• Similar to investigations, breach remediation is not something to avoid or learn on the job. First order of business is to stop the bleeding then figure out how the breach occurred. Additionally, depending on how bad the breach was, it is vital that the company consider the political impact of breach notification and the importance of doing it right.
Training	• Arrakis has numerous training courses available to train up your people to perform their security related job or increase their level of current training to improve productivity and overall security. Additionally, Arrakis can provide basic user level training.
Risk and Threat Assessments	• As a part of compliance, 3rd party risk and threat assessments should be done routinely. Depending on your risk you may consider performing this monthly. Arrakis has numerous highly trained professionals that can offload this for you.
Process Improvement	• Given the extensive amount of time Arrakis personnel have in the technology, security, and business areas, Arrakis can easily help point areas of improvement and what we can do to help.

Case Study: Security Assessments as a Service (SAaaS)

The client is a leading provider, for their business area, and has operations on a wide scale.

Arrakis and the client team-up to allow Arrakis to perform SAaaS as an unbiased 3rd party. The services include all aspects of a security assessment of a company respective of their size to insure that all policies, procedures, controls, and technologies are correctly used to protect the company and the companies data.

Problem	Solution	Outcome
• Rapidly changing or evolving threats • Demands for compliance • Internal security organization is young • High volume of technological use • High demand for assessments • Need for experience in security controls • Challenges dealing with 3rd parties	• Flexible level of service based on the needs of the client • Established process using a consistent methodology • Risk and Threat Assessment services that can be scaled to fit the need of the client • Vulnerability assessments, policy review, internal and external penetration testing, vendor risk assessments • Implement a solid process that is easily scalable for future needs	• Access to Arrakis resources that have the skills and knowledge to deal with threats • Increase speed of execution for deliverables to reduce risk. • Adaptable skillsets that allow for and adjust to a changing environment. • Transparency of all Arrakis involvement with the client. • Long term partnership with Arrakis that reduces the needs for continuous negotiation.

Case Study: Intelligence Services

The client is a person of popularity or influence where a negative image may impact their business, stock price, or professional influence in the circles the client revolves in. It is important to the client that negative influences in his/her life be minimized to a reduced and manageable situation.

Problem	Solution	Outcome
• The client is well known in the industry. • The client is a thought leader. • The client is worth over $50MM USD. • The client has had occasional newsworthy mishaps that have been a negative impact. • The client has had threats of blackmail as well as attempted KNR. • Any future mishaps will drastically impact the client in relation to social circles, stock prices, potential for future business, and influence in professional circles. • Overly negative incidents will cause the client to be shunned.	• Ensure a complete understanding of all new actors in the clients current and immediate future. • Ensure a reliable set of misinformation to misdirect adversaries of the client. • Ensure a solid counter-surveillance program is in place. • Train the client on basic misdirection, counter-surveillance, and situational awareness. • Ensure a solid protective plan is in place and provide reliable operational intelligence for PSD to increase safety. • Provide technology assets that increase the electronic security of the client.	• The client has increased freedom of movement without public knowledge. • The safety of the client is increased. • The client has more opportunities for secure communication. • The client has further knowledge of the nearby persons. • The client has increased awareness in business dealings. • Adaptable skillsets that allow for and adjust to a changing environment. • Long term partnership with Arrakis that reduces the needs for continuous negotiation.

World Wide range of capabilities and reach

Q/A?

For further information, please do not hesitate to contact sales@arrakisconsulting.com or make contact with your personal account manager.

Other interesting hyperlinks

General Company Presentation
Cybersecurity
Compliance and Audit
Stages of an Attack
Private Hosting Services
Hosting and other Services
Engineering, Architecture, and Design

Arrakis

LinkedIn
Facebook
Twitter