CYLANCE™
CONSULTING

PREVENTION AS A BUSINESS STRATEGY

BEN DENKERS
VP CONSULTING, NORTH AMERICA

SAFE HARBOR

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

THE PRESENTER

BEN DENKERS

VP Consulting, North America

- 15+ years of security experience in pen testing, incident response, forensics, and security consulting
- Served as Managing Director of Enterprise Security Services and Worldwide Managing Director of Red Team Services
- Really I just I like to hack stuff.

CYLANCE

AGENDA

Why services? Magento Bug:
What we know and impacts to businesses

Combating Magento

Evolving to Prevention

MAGENTO: BY THE NUMBERS

Magento is one of the largest open source e-commerce platform used by small retailers and big companies.

98
MILLION

Estimated number of online shoppers to be served by Magento merchants by 2020[1]

$155
BILLION

Gross merchandise volume transacted on the platform annually[2]

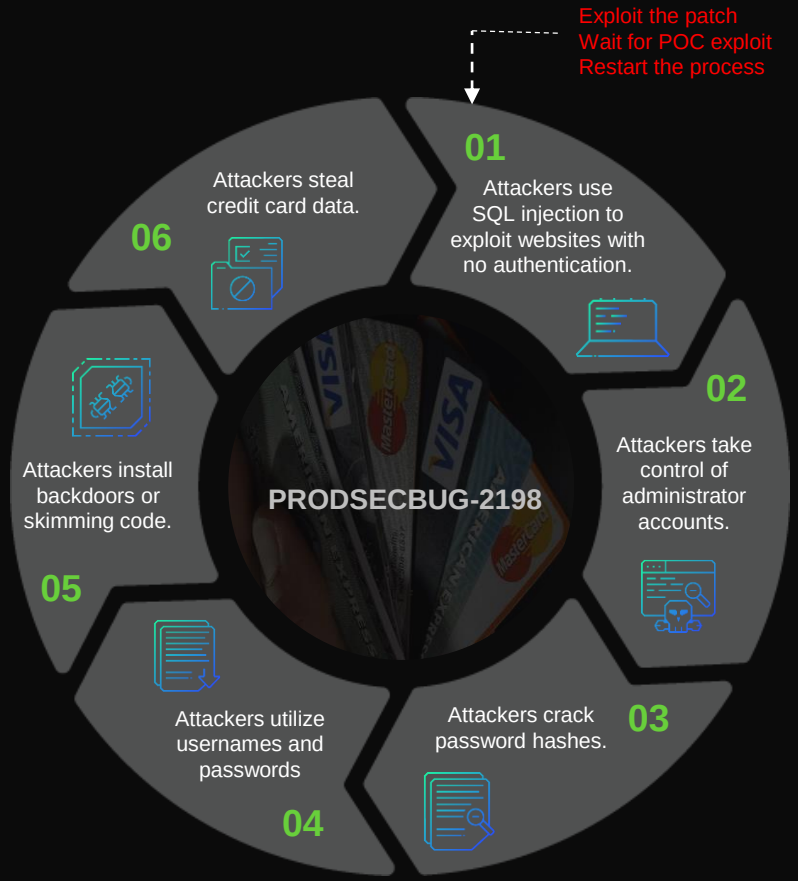
858K
WEBSITES

Number of customers that are Magento websites[3]

[1] https://magento.com/blog/magento-news/101-billion-digital-commerce-sold-merchants-using-magento-2016 / [2] https://magento.com/advantage / [3] https://trends.builtwith.com/shop/Magento

MAGENTO VULNERABILITY

- Has resided in Magento since version 1
- Unauthenticated and can be automated, resulting to more successful, widespread attacks against vulnerable websites
- **Cost and implications to victim companies?**



CYLANCE

WHY ARE THEY DOING IT

- Sheer volume of transactions done online today
- Payout from harvested credentials
- Can be automated and can be easily replicated

CYLANCE

COMBATING MAGENTO

How to protect your organization and prevent a similar attack in the future

CASE STUDY

- Client's website is hosted by a third-party in the EU
- Affected by an iframe replacement through XSS (SQLi)
- Occurred on an old module of the Magento platform (1.14.4.0) hosted on behalf of the client
- Affected Magento resource was **AjaxController.php**
- **500+ credit card form fills by EU citizens**

TIMEFRAME

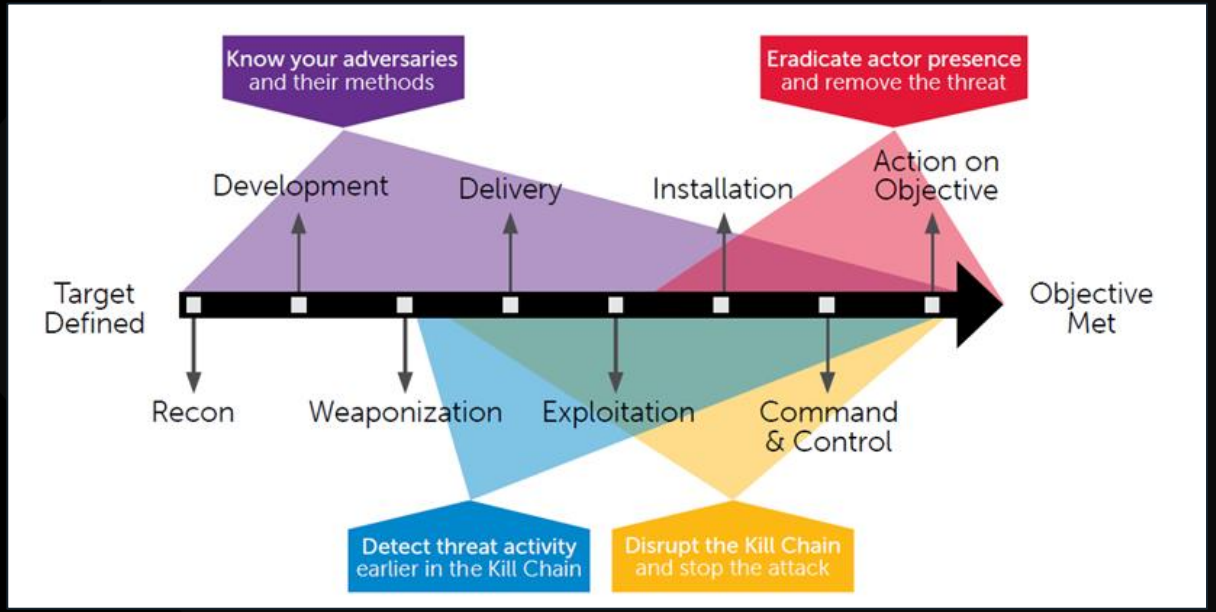
- **Patch +2 days - 17:04 - 17:08 UTC**: Time the threat actor injected malicious code; IP from Sweden.
- **Patch +2 days - 19:07 UTC:** Suspected time the threat actor had carried out attack.
- **Patch +2 days - 10:00 UTC:** Reported to the Client team.
- **Patch +2 days - 12:00 UTC:** Patch applied to webserver.

```
$sqlResults = $this->_connectionRead->fetchAll("SELECT city_name as placeName FROM " .
Mage::getSingleton('core/resource')->getTableName('localized_cities') . "
WHERE country = '" . $country . "' and city_zipcode = '" . $zipcode . "';");
```

THE CYBER KILLCHAIN

Phases

1. Reconnaissance
2. Development
3. Weaponization
4. Delivery
5. Exploitation
6. Installation
7. Command and Control
8. Action on Objective



CYLANCE

THWARTING DELIVERY

- Know your environment and current patch levels
- Have proper detection/prevention technologies in place
- Patch as soon as feasible
  - Utilize stopgaps until patch is implemented
- Check for lateral movement using a compromise assessment methodology or similar.

CYLANCE

EVOLVING TO PREVENTION

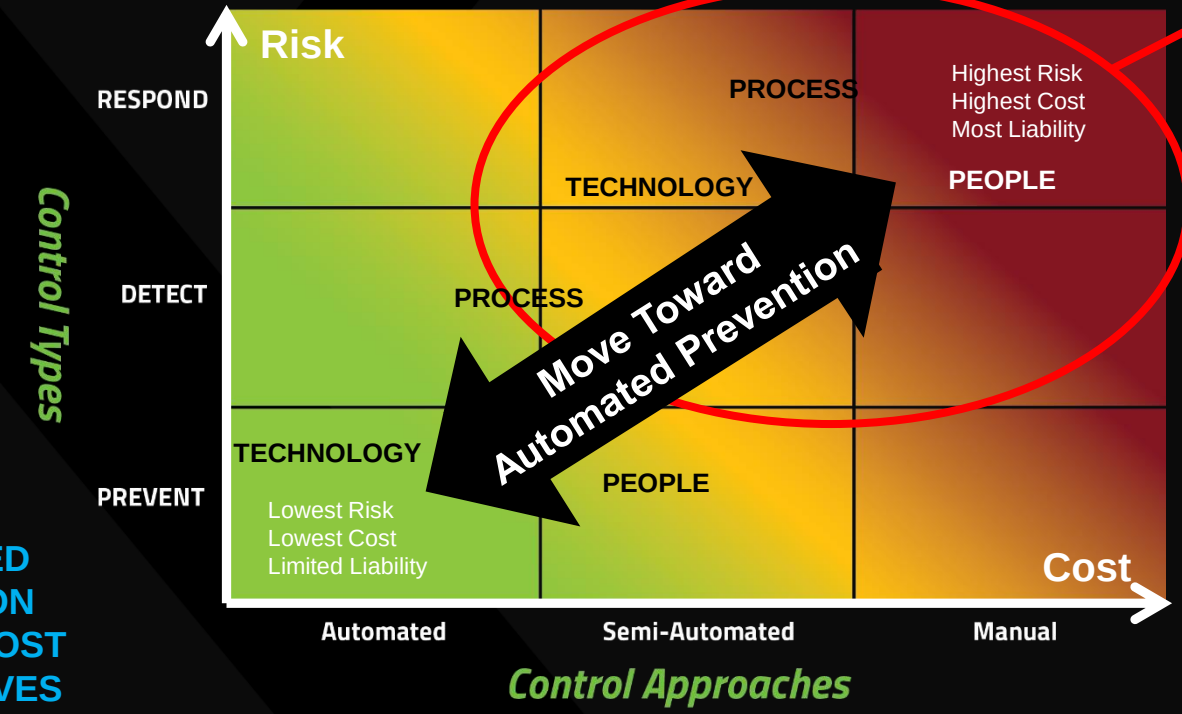
How to achieve perpetual prevention with the Cylance Prevention Platform

PATHWAY TO PREVENTION

Helping our clients move their environments into
a state of prevention from cyberattacks

CYLANCE™

GETTING TO AUTOMATED & MANAGED PREVENTION



Where Most Of The Industry Is Focused

AUTOMATED PREVENTION Takes your COST down & PROVES the ROI

What manual response technologies can you now REMOVE?

9–BOX OF CONTROLS

CYLANCE CONSULTING

CYLANCE PREVENTION PLATFORM™

CylancePROTECT®

Enterprise Prevention
Home Edition / MSSP

CylancePROTECT ®
with Optics™

Consistent Visibility
and Preventative EDR

ThreatZERO™
MANAGED PREVENTION

Managed Prevention
and Response

INCIDENT
CONTAINMENT

Remediate
Compromise

AI-BASED CONSULTING

Red Team | ICS | IoT/Embedded Systems

CYLANCE
CONSULTING

THE ASSESSMENT PARADOX

VULNERABILITY ASSESSMENTS

List of vulnerabilities

PEN TESTING

Anatomy of a hack

COMPROMISE ASSESSMENT

Are you hacked NOW?

CYLANCE

Deployment vs. Prevention

CYLANCE

Report Card

Grading Scale:

95 – 100% - A

94 – 85% - B

84 and Less - C

Files Analyzed	787,688,185
C	Overall Grade: 45.89%

Coverage Breakdown:

*Report generated as of 08/16/2016

Category	# Of Hosts/Files Under Category	Percentage Of Category	Description
Malware	5,374/7,098	75.71%	*The number of malware threats that have been quarantined.*
Potentially Unwanted Programs (PUPs)	22,067/34,259	64.41%	*The number of PUPs that have been quarantined/removed or whitelisted.*
Auto-Quarantine	543/13,452	4.04%	*The number of devices with Auto-Quarantine enabled for Unsafe and Abnormal threats.*
Memory Protection	0/13,452	0.00%	*The number of devices using Memory Protection in Block or Terminate mode.*
Script Control	0/13,452	0.00%	*The number of devices using Script Control in Block mode.*
Asset Inventory	11,644/13,452	86.56%	*The number of devices that have been online in the last 30 days.*
Upgrade Management	12,171/13,452	90.48%	*The number of devices on either of the two most recent versions of CylancePROTECT.*

CYLANCE

VALUE OF CYLANCEPROTECT

- AV ZERO – ROI Analysis
- PUPZERO
- Malware ZERO
- Memory Attacks ZERO
- Script Attacks ZERO

THREATZERO MANAGED PREVENTION

- Quarterly Prevention Assurance Reports
- Full malware status review
- Full PUP status review
- Updates of agent version
- Maintains your ThreatZERO status

CYLANCE

CYLANCE

Report Card

Grading Scale:

95 – 100% - A

94 – 85% - B

84 and Less - C

Files Analyzed	787,688,185
A	Overall Grade: 95.94%

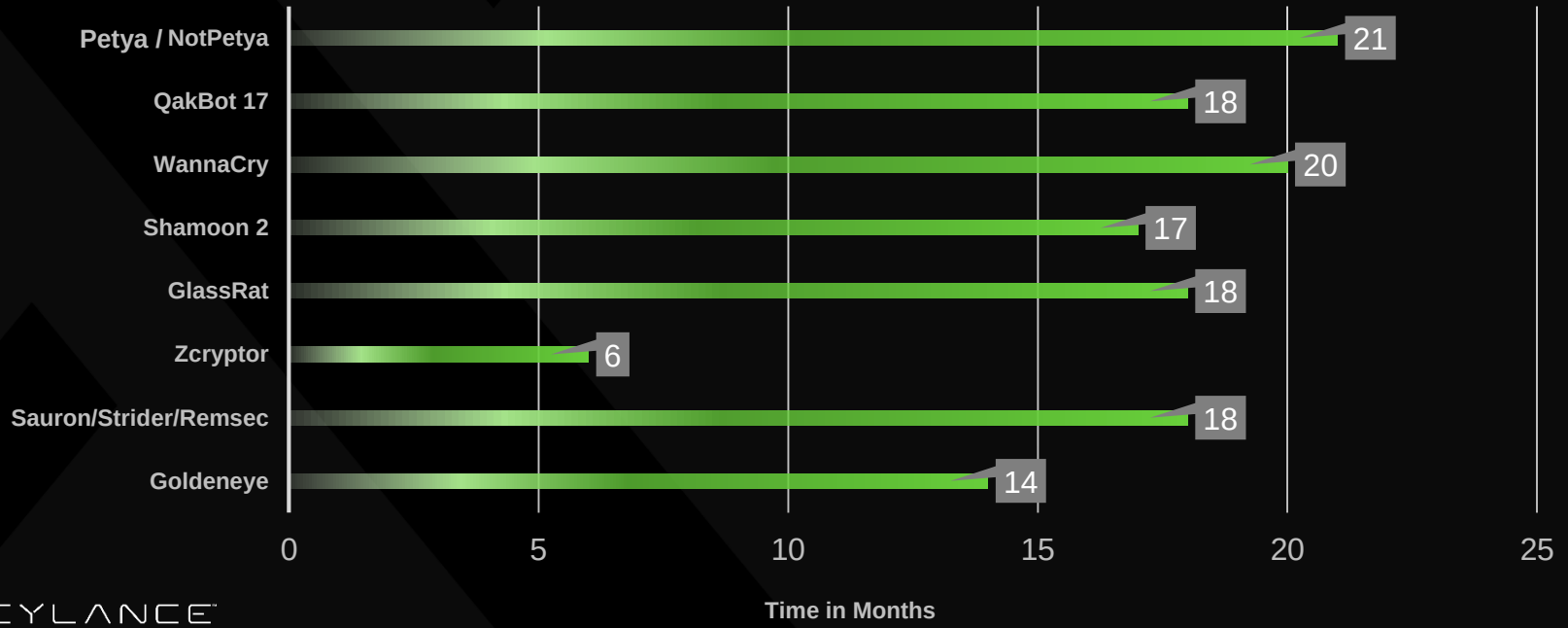
Coverage Breakdown:

*Report generated as of 08/16/2016

Category	# Of Hosts/Files Under Category	Percentage Of Category	Description
Malware	7,022/7,098	98.92%	*The number of malware threats that have been quarantined.*
Potentially Unwanted Programs (PUPs)	33,745/34,259	98.50%	*The number of PUPs that have been quarantined/removed or whitelisted.*
Auto-Quarantine	13,355/13,452	99.28%	*The number of devices with Auto-Quarantine enabled for Unsafe and Abnormal threats.*
Memory Protection	13,060/13,452	97.08%	*The number of devices using Memory Protection in Block or Terminate mode.*
Script Control	12,904/13,452	95.93%	*The number of devices using Script Control in Block mode.*
Asset Inventory	11,679/13,452	86.82%	*The number of devices that have been online in the last 30 days.*
Upgrade Management	12,783/13,452	95.03%	*The number of devices on either of the two most recent versions of CylancePROTECT.*

PREVENTION IS POSSIBLE

CylancePROTECT® has been able to detect and block new threats before they were first seen “in the wild” – without any updates or special configuration.



CYLANCE

DELIVERING PREVENTION-BASED SOLUTIONS

- Integrated Practice Areas
- Dedicated Engagement Manager
- Holistic Approach
- Customized Solutions
- World-Renowned Security Authorities
- Global Coverage with Local Attention

IoT / EMBEDDED SYSTEMS

INCIDENT CONTAINMENT & FORENSICS

INDUSTRIAL CONTROL SYSTEMS

RED TEAM SERVICES

ThreatZERO™

STRATEGIC SERVICES

EDUCATION

CYLANCE™

LET US PROVE IT TO YOU

IT'S ABOUT THE OUTCOME – PERPETUAL PREVENTION