Cyber Resiliency

Stop attacks before they start

Archis Gore,
CTO, Polyverse

www.polyverse.com

Polyverse - *Stop Attacks Before They Start*

Founded in 2015 we brought together top engineering talent from Microsoft, Amazon, Google and Open Source

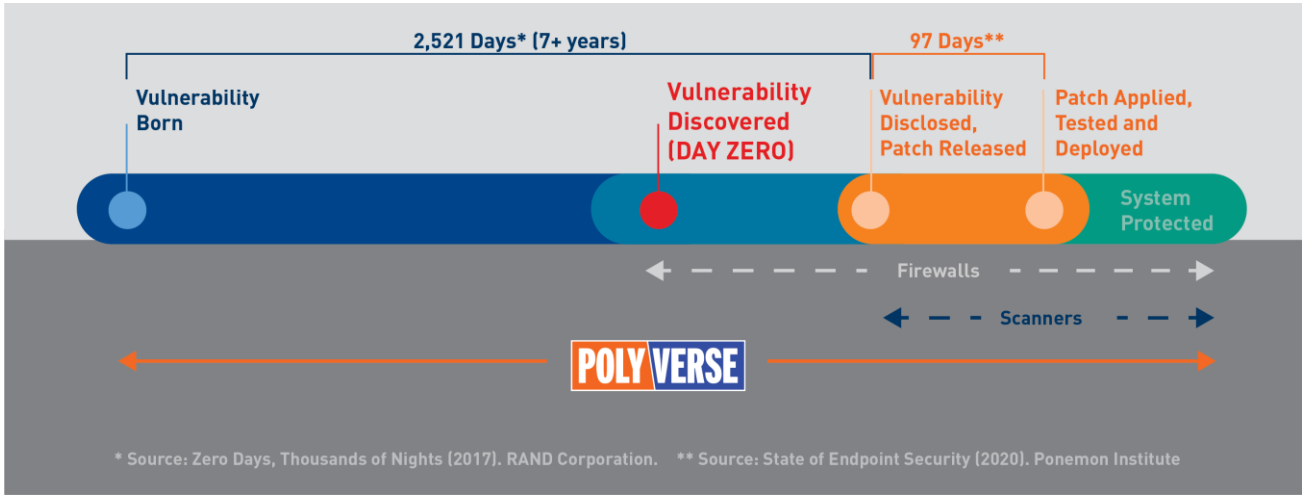
Traditional Cybersecurity = Reactive

Polyverse = Built in Cyber Resiliency

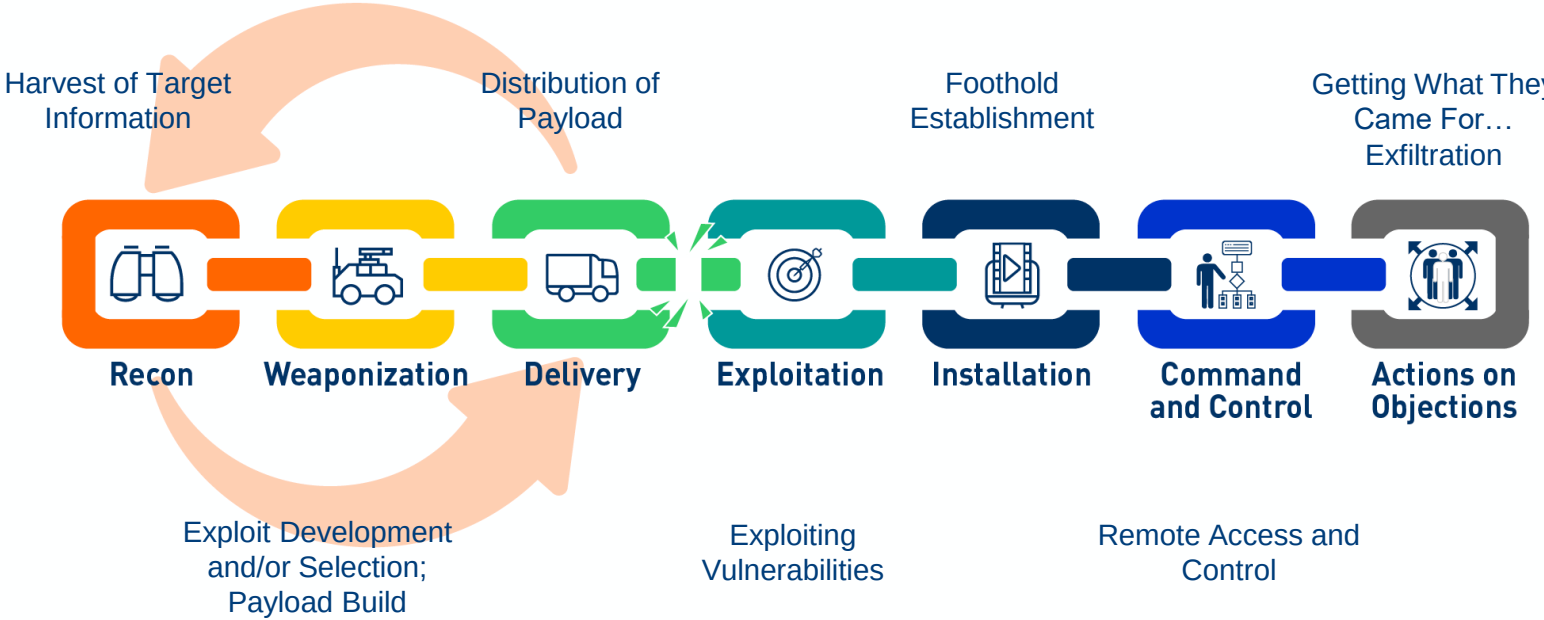
Our Mission is to solve cybersecurity problems once and for all.

Zero Trust Software: Assume the Bug

- Over 1 million unpatched vulnerabilities in Linux (Polyverse Linux Weakness Report)
- Average 97 days to deploy patches; many Zero-day exploits run for Years!
- Vulnerabilities can be accidental or intentional (solarwinds)
- Legacy and End-of-Life systems are particularly at risk



Polyverse Stops Attacks Before They Start



Polyverse takes away an attacker's assumptions when crafting an exploit, keeping them locked in the first 3 stages of the kill chain

Polyverse Zero Trust Software Solutions

Polymorphing for Linux

Unique Hardened Linux Repos that Stop Memory Based-Attacks

Secures the Linux estate stopping known and Zero-Day memory-based cyberattacks

- Teardrop
- Bluekeep
- WannaCry
- Spectre
- Meltdown
- Boothole
- Sudo

Available for -

- 25 Linux distros and versions
- Custom compile available

Polyscripting

Open Source PHP Hardening Using Polymorphic Language Technology

Secures websites, databases, etc. from script injection attacks

- Magecart
- DoD
- Equifax
- Mongo
- WordPress
- Yahoo
- eBay

Available via GitHub -

- For PHP
- WordPress

https://github.com/polyverse/php
https://github.com/polyverse/polyscripted-wordpress/

Zerotect

Open Source Zero-Day Attack Detection

Detects and reports Blind ROP (BROP) and other memory-based attacks

- Use as stand-alone solution or integrate into any SIEM, SOC or monitoring system
- Current integrations with
  - ArcSight
  - PagerDuty

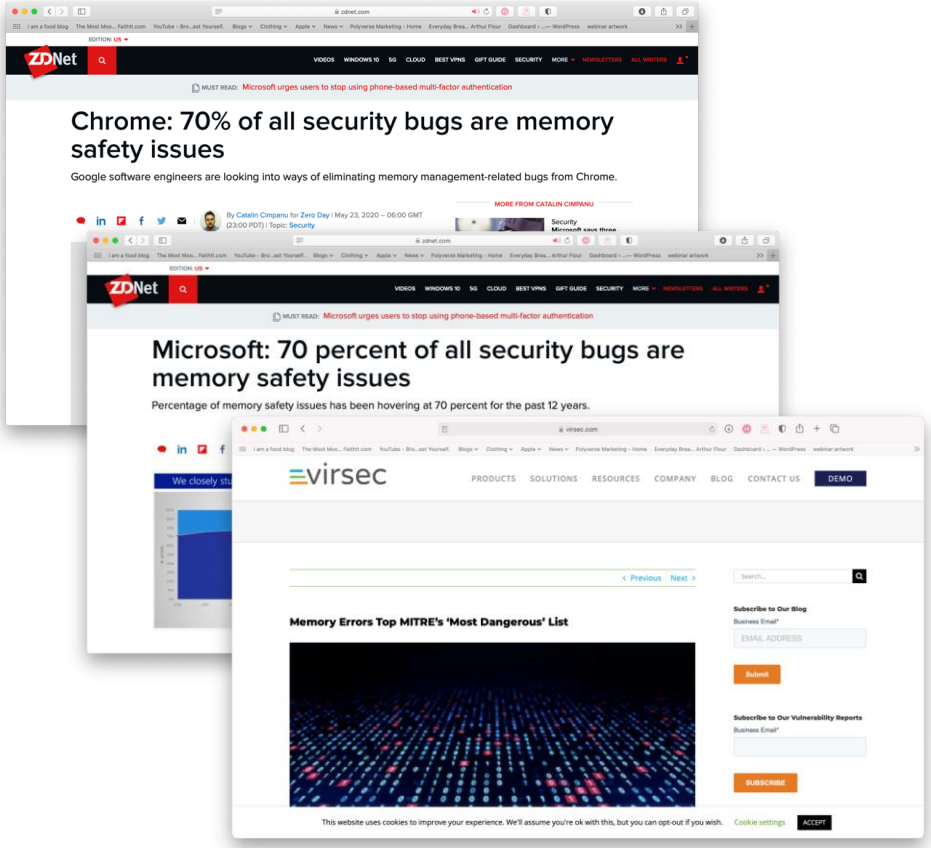
Available via GitHub

https://github.com/polyverse/zerotect

Polymorphing for Linux

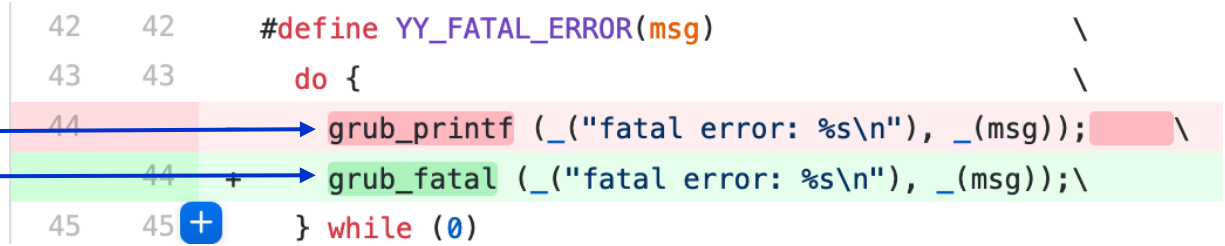
The world has a problem with Memory Safety…

- **Over 1M unpatched vulnerabilities**
- **identical versions of the OS** used
- **For an attacker, it's 'Break Once - Run Everywhere'**
- **>70% of vulnerabilities are memory-based which are the most lethal!**
  - WannaCry, Spectre, Meltdown, BlueKeep Ransomware



Happening right now: BootHole

May 5, 2010: Introduced
Apr 15, 2020: Upstream fix



```
42  42   #define YY_FATAL_ERROR(msg)                          \
43  43     do {                                               \
44         grub_printf (_("fatal error: %s\n"), _(msg));      \
       +   grub_fatal (_("fatal error: %s\n"), _(msg));\
45  45   } while (0)
```

July 30, 2020: NSA releases Cybersecurity Advisory on GRUB2 BootHole Vulnerability

* Cue panic patching, mitigations, opinion pieces in the tech press, etc. *

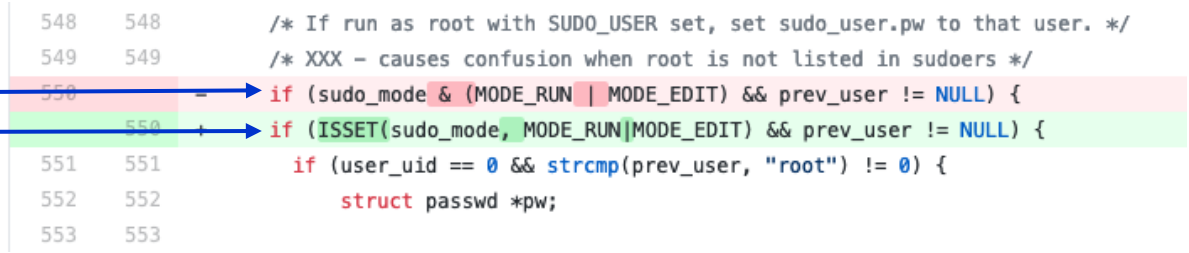
July 30, 2020: Ubuntu patches fail to boot: https://bugs.launchpad.net/ubuntu/+source/grub2/+bug/1889509

July 31, 2020: Red Hat's BootHole Patches Cause Systems to Hang ...

August 2017: Polyverse's Polymorphic distributions are born; mitigate attack string without knowledge of vulnerability existence.

Happening right now: Sudo privilege escalation

Oct 24, 2004: Introduced
Jan 23 2021: Upstream fix



```
548  548    /* If run as root with SUDO_USER set, set sudo_user.pw to that user. */
549  549    /* XXX - causes confusion when root is not listed in sudoers */
550       -  if (sudo_mode & (MODE_RUN | MODE_EDIT) && prev_user != NULL) {
     550  +  if (ISSET(sudo_mode, MODE_RUN|MODE_EDIT) && prev_user != NULL) {
551  551      if (user_uid == 0 && strcmp(prev_user, "root") != 0) {
552  552          struct passwd *pw;
553  553
```

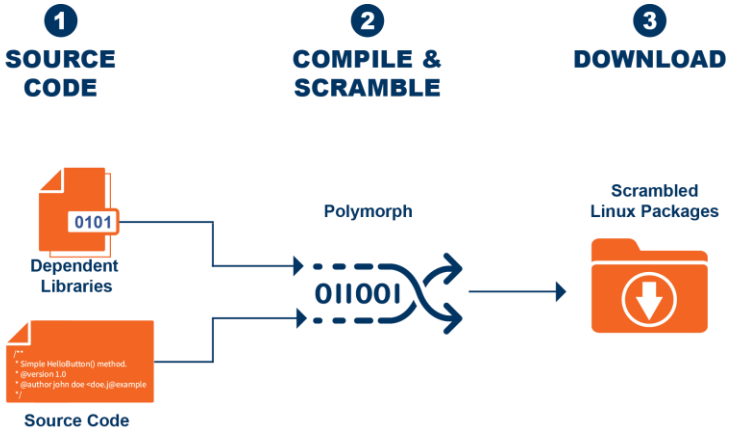
Jan 26, 2021: Qualys discloses to public: https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3

* Cue panic patching, mitigations, opinion pieces in the tech press, etc. *

August 2017: Polyverse's Polymorphic distributions are born; mitigate attack string without knowledge of vulnerability existence.

Polymorphing for Linux

- We compile and serve unique, hardened Linux repos (Channels) that stop attacks against memory-based vulnerabilities (>70%)
- SaaS delivery via annual subscription
- Single line of code installation
- Lightweight; works on 4MB IoT thru HPC Clusters
- Full support to Containers and Kubernetes
- *Deploy one or more Channels across the enterprise*
- 25 Linux Distros Currently Available
  - Alpine (v3.6 – v3.12)
  - CentOS (v6, v7, v8)
  - Debian (Stretch v9.0, Buster v10.0)
  - Fedora (v23, v24, v25)
  - RedHat (v6.x)
  - SUSE (v15.1, v15.2)
  - Ubuntu (Xenial v16.04, Bionic v18.04, Focal v20.04)
  - Amazon Linux (v1, v2)
  - Oracle (v6 v7)
- *Can compile and serve custom distros*



How?

- We change register allocation, PLT ordering, function addresses, init/fini block, expression evaluation and more, all at compile time
- Preserving semantics and functionality
- Stops attacker assumptions when crafting an attack = *The Attack Fails Every Time!*

Polymorphing: Install is under 10 minutes

Step 1: Backup your system

It's always good to make a backup, so if you spent time configuring your target environment we recommend you take a backup (host) or a snapshot (VM).

Step 2: Choose your operating system

CentOS (v6, v7 and v8)

Step 3: Update your OS

```
yum -y update
```

Step 4: Install Polyverse

If you have multiple authkeys, please choose the desired command below. To create more authkeys, please visit the Authkeys tab on the left.

```
curl https://repo.polyverse.io/cli | sh -s install [redacted]
```

Your packages are now scrambled and polyversed!

Step 5: Re-install your packages

```
yum -y update
```

```
yum -y reinstall \*
```

Polymorphing Creates Binary Diversity

```
void victim_function(size_t x) {
  if (x < array1_size) {
    temp &= array2[array1[x] * 512];
  }
}
```

Same source code goes through our build farm and compiles in multiple different ways to create unique versions of the OS

```
.cfi_startproc
pushq   %rbp
.cfi_def_cfa_offset 16
.cfi_offset 6, -16
movq    %rsp, %rbp
.cfi_def_cfa_register 6
movq    %rdi, -8(%rbp)
movl    array1_size(%rip), %eax
movl    %eax, %eax
cmpq    -8(%rbp), %rax
jbe     .L3
movq    -8(%rbp), %rax
addq    $array1, %rax
movzbl  (%rax), %eax
movzbl  %al, %eax
sall    $9, %eax
cltq
movzbl  array2(%rax), %edx
movzbl  temp(%rip), %eax
andl    %edx, %eax
movb    %al, temp(%rip)
```

```
        .cfi_startproc
        movl    array1_size(%rip),
%eax
        cmpq    %rdi, %rax
        jbe     .L1
        movzbl  array1(%rdi), %eax
        sall    $9, %eax
        cltq
        movzbl  array2(%rax), %eax
        andb    %al, temp(%rip)
.L1:
        rep ret
        .cfi_endproc
.LFE4882:
        .size   victim_function, .-
victim_function
        .section    .text.unlikely
.LCOLDE0:
        .text
.LHOTE0:
        .section    .text.unlikely
.LCOLDB1:
        .text
```

```
        .cfi_startproc
        jmp
        victim_function_isomorph
        .cfi_endproc
        .cfi_startproc
        movl    array1_size(%rip), %ebx
        cmpq    %rdi, %rax
        jbe     .L1
        movzbl  array1(%rdi), %ebx
        sall    $9, %ebx
        cltq
        movzbl  array2(%rax), %ebx
        andb    %al, temp(%rip)
.L1:
        rep ret
        .cfi_endproc
```

Polymorphing for Linux Benefits

- Protects for End-of-Life and legacy Linux distros (EL6.x)
- Provides protection during periods when you cannot or choose not to patch
- Stops memory-based attacks; nearly 70% of security vulnerabilities, including Zero-Day
- Zero runtime overhead or changes to your existing processes or interoperability

Polyscripting

Wordpress has a problem with Code Injection

Goes by many names...

- **Remote File Inclusions (RFI)**
- **Local File Inclusions (LFI)**
- **Remote Code Execution (RCE)**
- **Object Injection**
- **Backdoor**

Severe vulnerabilities patched in Facebook for WordPress Plugin

The worst bug leads to remote code execution, if exploited.

Two severe vulnerab

Disclosed by the Wo
the bugs impact Face
Official Facebook Pix

The plugin, used to c
and to monitor site tr

Critical Security Flaw in WordPress Plugin Allows RCE

Author:
Lindsey O'Donnell
July 29, 2020 / 12:32

2 minute read

Buggy WordPress plugin exposes 100K sites to takeover attacks

By Sergiu Gatlan

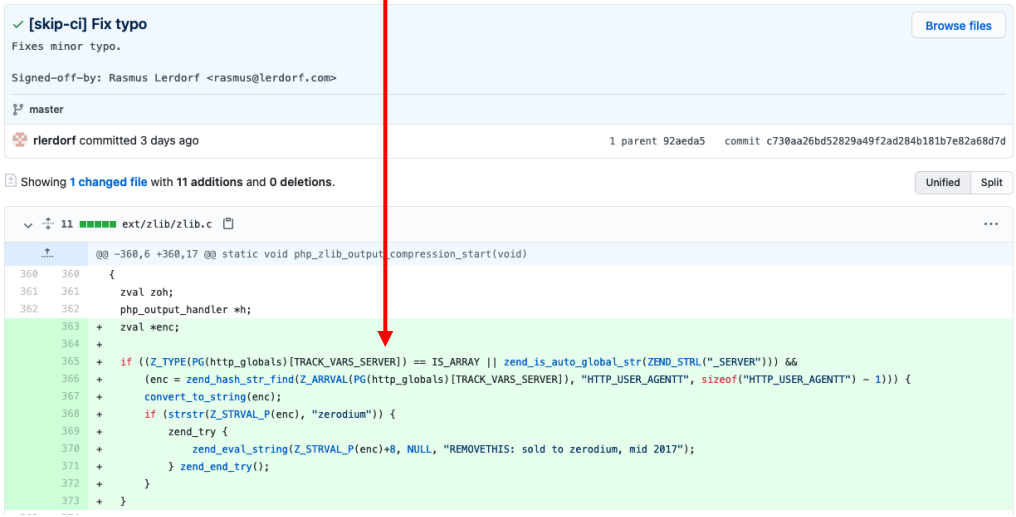
February 11, 2021 12:05 PM 0

Critical and high severity vulnerabilities in the Responsive Menu WordPress plugin exposed over 100,000 sites to takeover attacks as discovered by Wordfence.

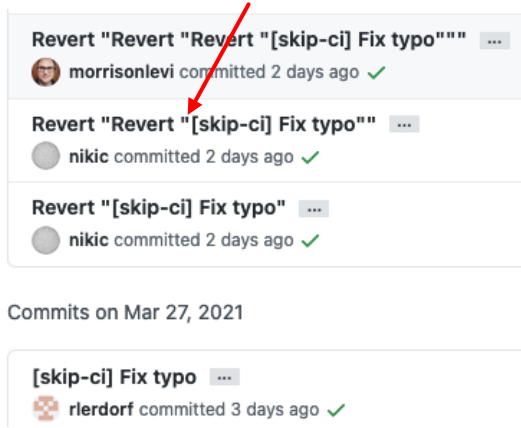
Responsive Menu is a WordPress plugin designed to help admins create W3C compliant and mobile-ready responsible site menus.

Happening right now: PHP Backdoor injection

Backdoor injected on Git Server March 27th 2021



Attackers attempted to revert the revert of their attack March 28th 2021



November 2018: Polyverse's Polyscripted PHP is Open Source and mitigates attack string without knowledge of vulnerability existence.

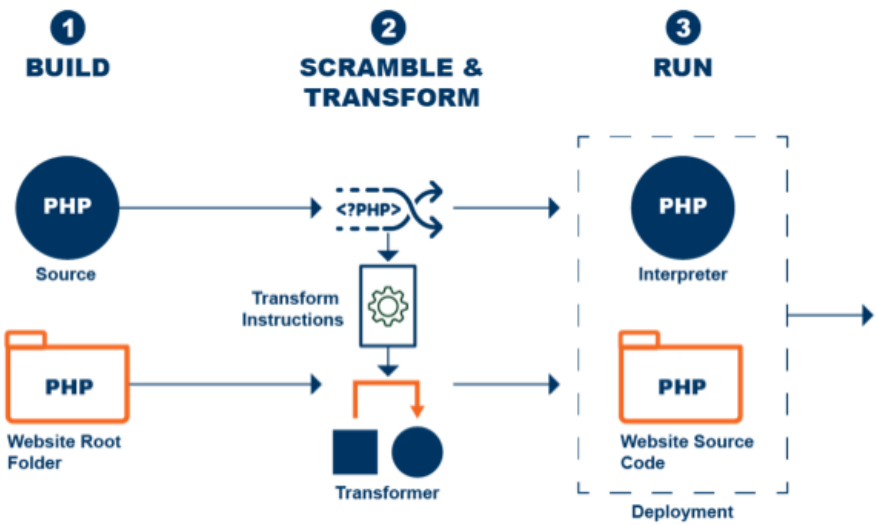
Polyscripting for PHP and Wordpress

Open Source security for PHP and WordPress

- Stops code injection attacks from executing
- Scrambles syntax and grammar of PHP
- Prevents non-approved code from running; introduced via
  - Backdoors
  - Remote code executions
  - File Inclusions
- Zero changes to source code
- Zero impact to program functionality or interoperability
- Zero performance overhead

Open Source available via Github

https://github.com/polyverse/php
https://github.com/polyverse/polyscripted-wordpress/



How?

- Each server website uses a unique instance of a translated scripting language.
- The server is unable to execute injected code
- Result: The attack vector is rendered ineffective.

Polyverse Polyscripting: Before and After

```
switch ($i)
{
    case "apple":
        echo "i is apple";
        break;
    case "bar":
        echo "i is bar";
        break;
    case "cake":
        echo "i is cake";
        break;
}
```

```
yEmP ($i)
{
    lScQJGp "apple":
        vKbarGE "i is apple";
        hRMxBL;
    lScQJGp "bar":
        vKbarGE "i is bar";
        hRMxBL;
    lScQJGp "cake":
        vKbarGE "i is cake";
        hRMxBL;
}
```

Polyscripting for PHP Benefits

Open Source

Provides protection against all code injections

Traps and Detects attacker

Zero runtime overhead

Zerotect

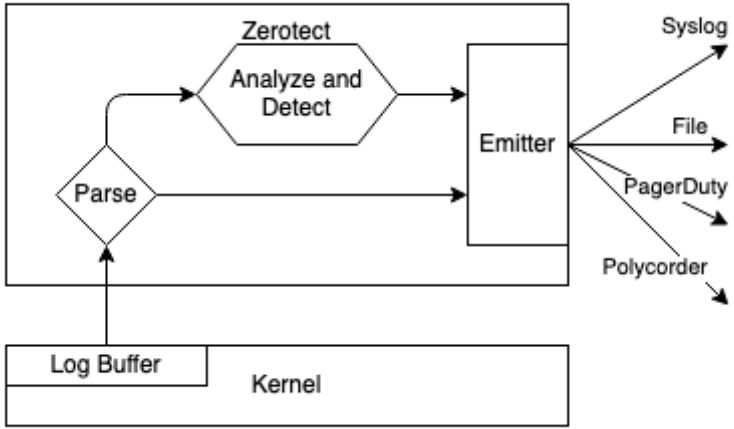
Zerotect

Open Source zero-day attack detector

- Interprets raw text-based kernel logs into structured logs for better analytics
- Built-in analytics for conclusive detection
- Does not interfere with system operations
- Integrates with all Monitoring, SIEM, SOC, Analytics, AI/ML tools.
- Certified by:
  - Micro Focus ArcSight
  - PagerDuty

Open Source available via Github

https://github.com/polyverse/zerotect



Zerotect Benefits

- Open Source
- Integrates with any SIEM, Monitoring, Analytics, AI/ML platform
- Interprets text-based logs into structured entries for analytics
- Performs minor analytics and detection on the client

Polyverse Customers & Partners

Polyverse Defense and Federal Engagement

- US Navy – Protecting critical systems throughout the fleet

- US CYBERCOM - Program support

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- Evaluating Polyverse Solutions

Polyverse Supported Compliance Frameworks

CIS Security Controls "SANS Top 20"

- **8.1:** Manage anti-malware software
- **8.2:** Ensure software signatures
- **8.3:** Enable OS anti-exploitation features
- **8.6:** Centralize anti-malware logging
- **11.3:** Automate standard configuration
- **11.4:** Install latest security updates
- **18.7:** Apply static code analysis tools
- **18.10:** Deploy web application firewalls

CMS Acceptable Risk Safeguards

- **CM-11:** Prohibit malicious software install
- **SI-3:** Malicious code protection
- **SI-3(1):** Central management
- **SI-3(2):** Automatic updates
- **SI-16:** Memory protection

FEDRAMP

- **AU-12**
- **CM-11:** User-installed software
- **SI-3:** Malicious code protection (Subsection 1, 2, 7)
- **SI-4:** Information system monitoring (Subsection 1, 24)
- **SI-16:** Memory protection

HIPAA

- 164.308(a)(5)(i)
- 164.308(a)(5)(ii)(B)

AICPA

- **CC5.8:** Prevent or detect malicious code
- **CC6.1:** Protect against known vulnerabilities

CRR V2016

- **VM:G1.Q3:** Malicious code detection tools
- **VM:G2.Q6:** Record vulnerability resolution
- **VM:G3.Q1:**Manage vulnerability exposure

CSA Cloud Controls Matrix v3.0.1

- **v3.0.1** MOS-17
- **v3.0.1** TVM-01

HITRUST Framework v1

- 03.c Risk mitigation
- 09.aa Audit logging
- 09.ae Fault logging
- 09.j Anti-malware
- 10.b Input data validation
- 10.c Control of internal processing
- 10.k Change control procedures
- 10.m Technical vulnerabilities
- 11.a Security event reporting
- 11.b Security weakness reporting
- 11.d Learning from incidents

State of Nevada – SPI (NRS 603A)

- NRS 603A.215.1

Massachusetts Data Protection Act

- 201 CMR 17.04(7)

COBIT

- COBIT 4.1 (DS5.9)
- COBIT 5 (DSS05.01)

PCI DSS v3.2

- Reference 5.1 (5.1.1, 5.1.2)
- Reference 5.2
- Reference 5.3

TX Health Services Code (TX HB 300)

- 181.004(a)

Title 1 TX Admin. Code 390.2

- 1 TAC 390.2(a)(1)
- 1 TAC 390.2(a)(4)(A)(xi)

ISO/IEC 27002:2005

- 10.4.1

ISO/IEC 27002:2013

- ISO/IEC 27002:2013 (12.2.1)
- ISO/IEC 27002:2013 (12.6.2)

IRS Publication 1075 v2014

- 9.3.17.10
- 9.3.17.3
- 9.3.17.4

MARS-E v2

- DM-2
- PE-2
- SC-2
- SI-3
- SI-3(1)
- SI-3(2)
- SI-3(7)
- SI-8
- SI-8(1)
- SI-16

NIST Critical Infrastructure v1

- DE.CM-4
- PR.AC-4
- PR.AT-1

NIST SP 800-53 R5

- CM-11
- SC-2
- SI-16
- SI-3
- SI-3(1)
- SI-3(2)

ISO 27799:2008

- 7.7.4.1

Where Polyverse Leads

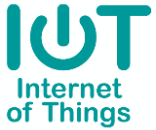
Used by the DoD
to protect critical assets.

Zero Impact Performance
tested and verified by Mitre, Disa.

Used on Over 1.2M
Servers Worldwide.

LegalShield
Used by largest global legal services company.

Protects Enterprise Linux Distributions
And ISV certified applications such as SLES, RHEL.



Only Cybersecurity Solution
that can run on 4MB IoT devices.

Sole Source Procurement Options
Product (Federal)

Spectre: #1 Protection
For variant 2.

CNBC Top 100
Startups in The World.*

https://www.cnbc.com/2019/11/12/polyverse-cnbc-upstart-100.html