Анализ атомов[1] AV.

Показан пример анализа атомов в **AV**. В данном тесте не используется код самих **AV**, а только результат тестирования в виде сигнатурного детекта. В следствие этого за один тест может быть проверено одно булево условие.

Как было сказано ранее, в **VM** код **API** содержит атомы, которые служат шлюзами **VM**. Через них управление получает **VM** и эмулирует **API**, которые не могут быть выполнены без использования среды **VM**. Простые **API** в свою очередь атомов не содержат.

Для тестов используется конструктор(это мотор, который описывает графом код и может собирать код по графу). Это не обязательно для подобных тестов, просто использовано для удобства.

Для детекта шифрованный образ **PE** декриптуется, выгружается в файл и запускается. Для примера взят ***Glyn***. Так как не все **AV** его детектят, то для теста других **AV** следует взять иной образ.

В начале запустим непосредственно декриптор, но после переноса тела **API** в буфер. Данная манипуляция выполняется конструктором. При этом используется вызов аллокатора, в качестве которого используется **VirtualAlloc()**. Код конструктора содержит стандартный набор инструкций и не использует системные механизмы(ничего не вызывает вне себя). Это уменьшает его влияние на тесты. Для успешного прохода данного кода **AV** должен эмулировать аллокатор.

Конструктор пересобирает код **API** в буфер. Затем этот буфер исполняется, результат исполнения является ключём к декрипту образа. Для тестов взята сложная функция — **GetProcAddress()**. Результат теста(C1):

Анализ | Сведения о файле | Дополнительные сведения | Комментарии | Голосование | Поведение

Антивирус	Результат	Дата обновления
ALYac	Win32.Glyn.A	20170219
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Win32.Glyn.A	20170219
Arcabit	Win32.Glyn.A	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
BitDefender	Win32.Glyn.A	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
ESET-NOD32	probably unknown NewHeur_PE	20170219
Emsisoft	Win32.Glyn.A (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Win32.Glyn.A	20170219

1 DFG: Защита потока данных(*Data Flow Guard*).

Как сказано выше в тест не включены **AV**, которые не содержат детект на образ и которые не смогли пройти тестовый код. В буфере код выполнен успешно. Определим число инструкций, из которых состоит тело **API**. Общее число их описано в графе. Получить его мы не можем, поэтому используем условную конструкцию к заданием возможного числа. Если условие верно(число инструкций < 10), то результатом будет детект(C2):

Анализ | Сведения о файле | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Gen:Trojan.Heur.GZ.bmW@bm7PGHg	20170219
Arcabit	Trojan.Heur.GZ.ECD7E7	20170219

Только ***AVG*** содержит < 10 инструкций в теле этой функции. Увеличим значение до 32(C3):

Анализ | Сведения о файле | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
ALYac	Win32.Glyn.A	20170219
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Win32.Glyn.A	20170219
Arcabit	Win32.Glyn.A	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
BitDefender	Win32.Glyn.A	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
ESET-NOD32	probably unknown NewHeur_PE	20170219
Emsisoft	Win32.Glyn.A (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Win32.Glyn.A	20170219

Видно что остальные **AV** содержат более 10 инструкций. Далее определим структуру кода – наличие в нём ветвлений. Пройдя по всем инструкциям графа найдём ветвления(за исключением инструкции возврата **Ret**) и при их обнаружении выдадим детект(C4):

Emsisoft	Gen:Trojan.Heur.GZ.bmW@bKktDOf (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Gen:Trojan.Heur.GZ.bmW@bKktDOf	20170219
GData	Gen:Trojan.Heur.GZ.bmW@bKktDOf	20170219
Ikarus	Virus.Win32.Glyn	20170219

Только ***Ikarus*** содержит не линейный код(с ветвлениями). Уточним число инструкций, увеличив лимит до 96(C3i). Результат тот же. Эта **API** является сложной реализацией.

Определим какие ветвления присутствуют в данной **API** у ***Ikarus***(C4i). Перечислив все типы ветвлений, остаётся одно безусловное процедурное ветвление(Call rel).

В теории были описаны способы изоляции выборки данных(**DF**). Простейший способ обнаружить **DF** – расширение стека при доступе к сторожевой странице. Из атомов таких обращений нет(если не эмулируются намеренно) — он изолирован от эмулируемой среды. Выполним вызов атома, передав ссылку на гвард страницу стека: После возврата из **API** проверим стек на расширение и если он не расширен, то выдадим детект(C5).

Анализ | Сведения о файле | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
ALYac	Win32.Glyn.A	20170219
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Win32.Glyn.A	20170219
Arcabit	Win32.Glyn.A	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
BitDefender	Win32.Glyn.A	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
ESET-NOD32	probably unknown NewHeur_PE	20170219
Emsisoft	Win32.Glyn.A (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Win32.Glyn.A	20170219

Изменим условие проверки на обратное для наглядности(C5e)..

Endgame	malicious (moderate confidence)	20170217
F-Secure	Gen:Trojan.Heur.GZ.bmW@b4mU5ih	20170219
GData	Gen:Trojan.Heur.GZ.bmW@b4mU5ih	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219
eScan	Gen:Trojan.Heur.GZ.bmW@b4mU5ih	20170219
Qihoo-360	HEUR/QVM19.1.0000.Malware.Gen	20170219

Проверим расширение стека непосредственно на инструкциях, что бы узнать поддерживается ли данный механизм. Обратимся напрямую к сторожевой странице и при расширении стека выдадим детект(C6). ***Ikarus*** данный механизм не поддерживает. Только ***Kaspersky*** выполняет расширение стека **API**. В таком случае выполняется доступ из тела **API** к её аргументу, либо стек расширяется при валидации указателей в **VM**(намеренно):

Антивирус	Результат	Дата обновления
ALYac	Win32.Glyn.A	20170219
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Win32.Glyn.A	20170219
Arcabit	Win32.Glyn.A	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
BitDefender	Win32.Glyn.A	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
ESET-NOD32	probably unknown NewHeur_PE	20170219
Emsisoft	Win32.Glyn.A (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Win32.Glyn.A	20170219
GData	Win32.Glyn.A	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219
eScan	Win32.Glyn.A	20170219

Разложить код на трассу можно тремя путями — машинной трассировкой(**TF**), эмуляцией или динамической эмуляцией(**DYE**). Выполним(C7) это что бы получить доступ к атому(далее можно его исследовать непосредственно)..

Анализ | Сведения о файле | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Gen:Trojan.Heur.GZ.bmW@bul2Xmj	20170219
Arcabit	Trojan.Heur.GZ.ED4C7D	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9602	20170217
BitDefender	Gen:Trojan.Heur.GZ.bmW@bul2Xmj	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
Emsisoft	Gen:Trojan.Heur.GZ.bmW@bul2Xmj (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Gen:Trojan.Heur.GZ.bmW@bul2Xmj	20170219
GData	Gen:Trojan.Heur.GZ.bmW@bul2Xmj	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219

Функция трассирована через элементарный **DYE**-цикл. Детекты **BitDefender** и его клонов исчезли. Из этого следует что его атомы привязаны к положению частей кода, либо состоят не из одной инструкции, так как при выполнении атома в буфере эмуляция прекращается, убедимся в этом вставив после возврата из цикла **DYE** прямой вызов декриптора(C8):

AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Gen:Trojan.Heur.GZ.bmW@b8v4M@f	20170219
Arcabit	Trojan.Heur.GZ.EA22A3	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9521	20170217
BitDefender	Gen:Trojan.Heur.GZ.bmW@b8v4M@f	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
Emsisoft	Gen:Trojan.Heur.GZ.bmW@b8v4M@f (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Gen:Trojan.Heur.GZ.bmW@b8v4M@f	20170219
GData	Gen:Trojan.Heur.GZ.bmW@b8v4M@f	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219
eScan	Gen:Trojan.Heur.GZ.bmW@b8v4M@f	20170219
Qihoo-360	HEUR/QVM19.1.0000.Malware.Gen	20170219

Определим номер инструкции, которая является атомом. Этим событием является возврат из атома и соответственно возврат значения в регистр. Зададим для примера минимальное значение в 5 итераций(C9):

Антивирус	Результат	Дата обновления
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Gen:Trojan.Heur.GZ.bmW@bKyLoYg	20170219
Arcabit	Trojan.Heur.GZ.E3D802	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9574	20170217
BitDefender	Gen:Trojan.Heur.GZ.bmW@bKyLoYg	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
Emsisoft	Gen:Trojan.Heur.GZ.bmW@bKyLoYg (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Gen:Trojan.Heur.GZ.bmW@bKyLoYg	20170219
GData	Gen:Trojan.Heur.GZ.bmW@bKyLoYg	20170219
Invincea	generic.a	20170203
eScan	Gen:Trojan.Heur.GZ.bmW@bKyLoYg	20170219

У **AVG** атом расположен на 5-й инструкции. Передадим инвалидный указатель в атом, прежде зарегистрируем ловушку(**SEH**) и при срабатывании ловушки выведем детект(C11):

Анализ | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Gen:Trojan.Heur.TP.bmW@bmL0fLo	20170219
Arcabit	Trojan.Heur.TP.EDAF04	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9509	20170217
BitDefender	Gen:Trojan.Heur.TP.bmW@bmL0fLo	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
Emsisoft	Gen:Trojan.Heur.TP.bmW@bmL0fLo (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Gen:Trojan.Heur.TP.bmW@bmL0fLo	20170219
GData	Gen:Trojan.Heur.TP.bmW@bmL0fLo	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219

AVG и **Kaspersky** разворачивают исключение при обнаружении инвалидного указателя. Обернём вызов **API** в **SEH** и передадим инвалидный указатель(C12):

Антивирус	Результат	Дата обновления
ALYac	Win32.Glyn.A	20170219
AVG	Win32/Glyn.dropper	20170219
Ad-Aware	Win32.Glyn.A	20170219
Arcabit	Win32.Glyn.A	20170219
Avast	Win32:Evo-gen [Susp]	20170219
Avira (no cloud)	TR/Crypt.ZPACK.Gen	20170219
BitDefender	Win32.Glyn.A	20170219
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
ESET-NOD32	probably unknown NewHeur_PE	20170219
Emsisoft	Win32.Glyn.A (B)	20170219
Endgame	malicious (high confidence)	20170217
F-Secure	Win32.Glyn.A	20170219
GData	Win32.Glyn.A	20170219
Invincea	generic.a	20170203
Kaspersky	Virus.Win32.Glyn	20170219
eScan	Win32.Glyn.A	20170219

Появляется детект **BitDefender**, таким образом он не разворачивает исключение, а возвращает управление из атома. Интересно определить какой адрес передаётся в ловушку..

Касперский расширяет стек из атомов, но можно исследовать его на несколько выборок данных за один вызов, расположив указатели в разных страницах стека и выбрав **API** с несколькими указателями.

Показан принцип исследования тела апи/атомов. Можно исследовать другие **AV**(к примеру ***VBA*** и ***Yandex*** так же успешно проходят пересборку и аллокатор).

Путём деления булевого условия может быть выполнено чтение тела **API**(подобно как у бинарных деревьев). Но такое чтение требует множество итераций.