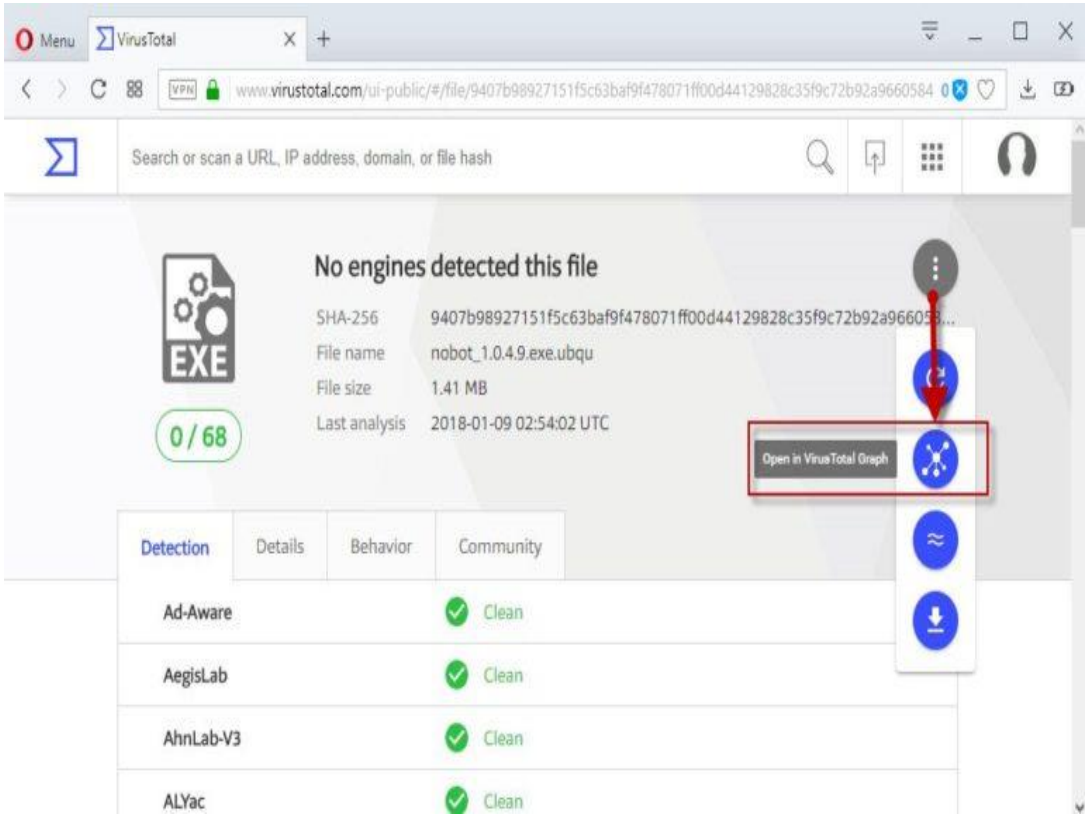
بسمه تعالی

# مشاهده‌ی آسان بدافزار با استفاده از ویژگی جدید گراف‌سازی VirusTotal

گراف‌سازی ویژگی جدیدی از VirusTotal است که ارتباط بین فایل‌ها، URLها، دامنه‌ها و آدرس‌های IP هر مجموعه‌داده‌ی تجزیه و تحلیل‌شده را نشان می‌دهد. VirusTotal سرویس مفیدی است که به هر کاربر اجازه می‌دهد فایل‌ها را بارگذاری کند و آن‌ها را با استفاده از بیش از ۶۰ موتور آنتی‌ویروس مختلف بررسی نماید.

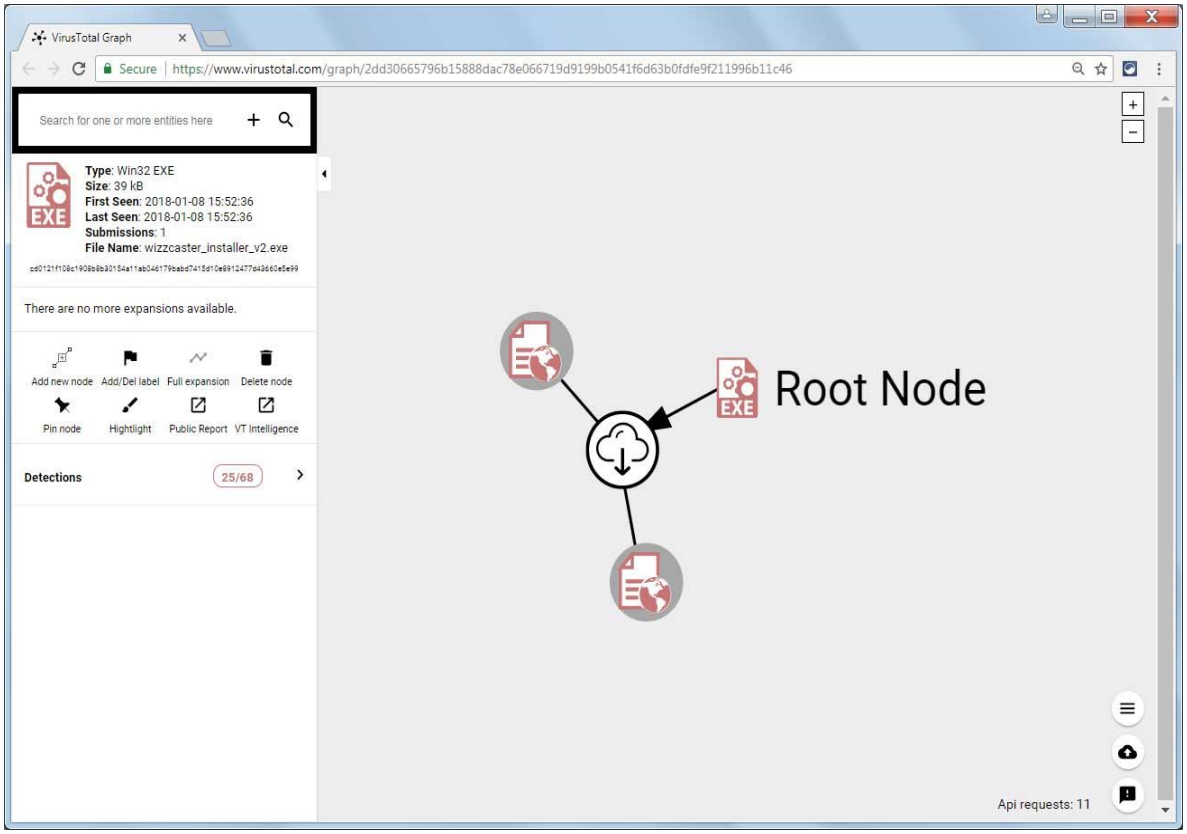
ابزار جدید VirusTotal تنها در دسترس مشترکین VirusTotal نیست و تمامی اعضا می‌توانند از آن استفاده کنند.

این گراف را می‌توان مستقیماً از آدرس https://www.virustotal.com/graph/ و ارایه‌ی هش شناخته‌شده یا رفتن به صفحه‌ی تجزیه‌وتحلیل یک فایل خاص به‌دست آورد. در صفحه‌ی تجزیه‌وتحلیل، گزینه‌ی جدیدی در فهرست با عنوان Open in VirusTotal Graph وجود دارد که کاربر را به صفحه‌ی گراف می‌برد (شکل ۱).




**شکل ۱ دسترسی به گراف ارایه‌شده**

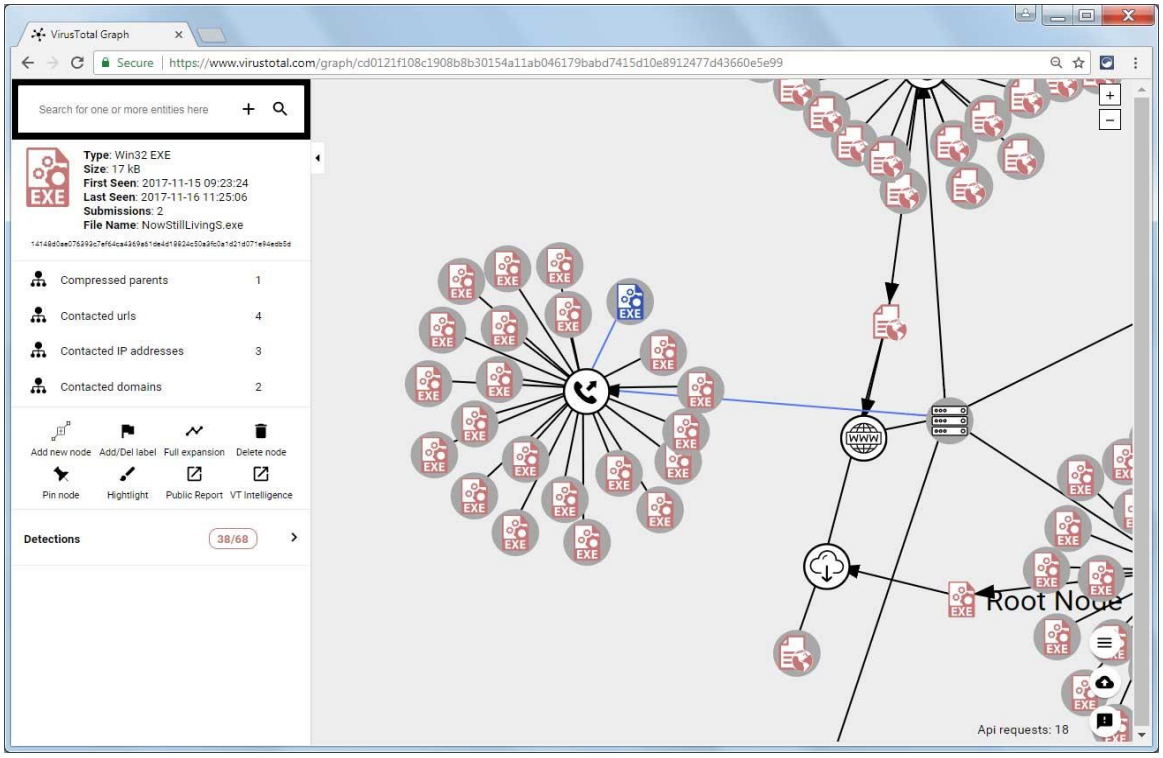
همان‌طور که در شکل ۲ مشاهده می‌شود، در صفحه‌ی گراف، عنصری به نام Root Node (گره ریشه) مشاهده می‌شود. این عنصر شئ مرتبط با فایلی است که به VirusTotal تحویل داده شده است. از این گره، پیکان‌های مختلفی به اطلاعات مربوط به این نمونه مشاهده می‌شود.




**شکل ۲ صفحه‌ی VirusTotal Graph**

در این گزارش، گراف ساده‌ی مربوط به یک تبلیغ‌افزار موردبررسی قرار خواهد گرفت. این گراف شامل گره ریشه و دو آدرسی  است که به آن‌ها متصل می‌شود.

کاربر می‌تواند بر روی هر گره دوبارکلیک کند تا اطلاعات بیشتری را درباره‌ی آن شئ‌داده‌ای خاص به‌دست آورد. هنگامی‌که بر روی یک گره دوبارکلیک می‌شود، آن شئ را گسترده می‌کند و داده‌های مربوط به آن شئ را نمایش می‌دهد. در شکل ۳ فایل‌هایی که توسط گره ریشه (Root Node) در زمان اتصال آن به یک آدرس دانلود شده‌اند، مشاهده می‌شود.

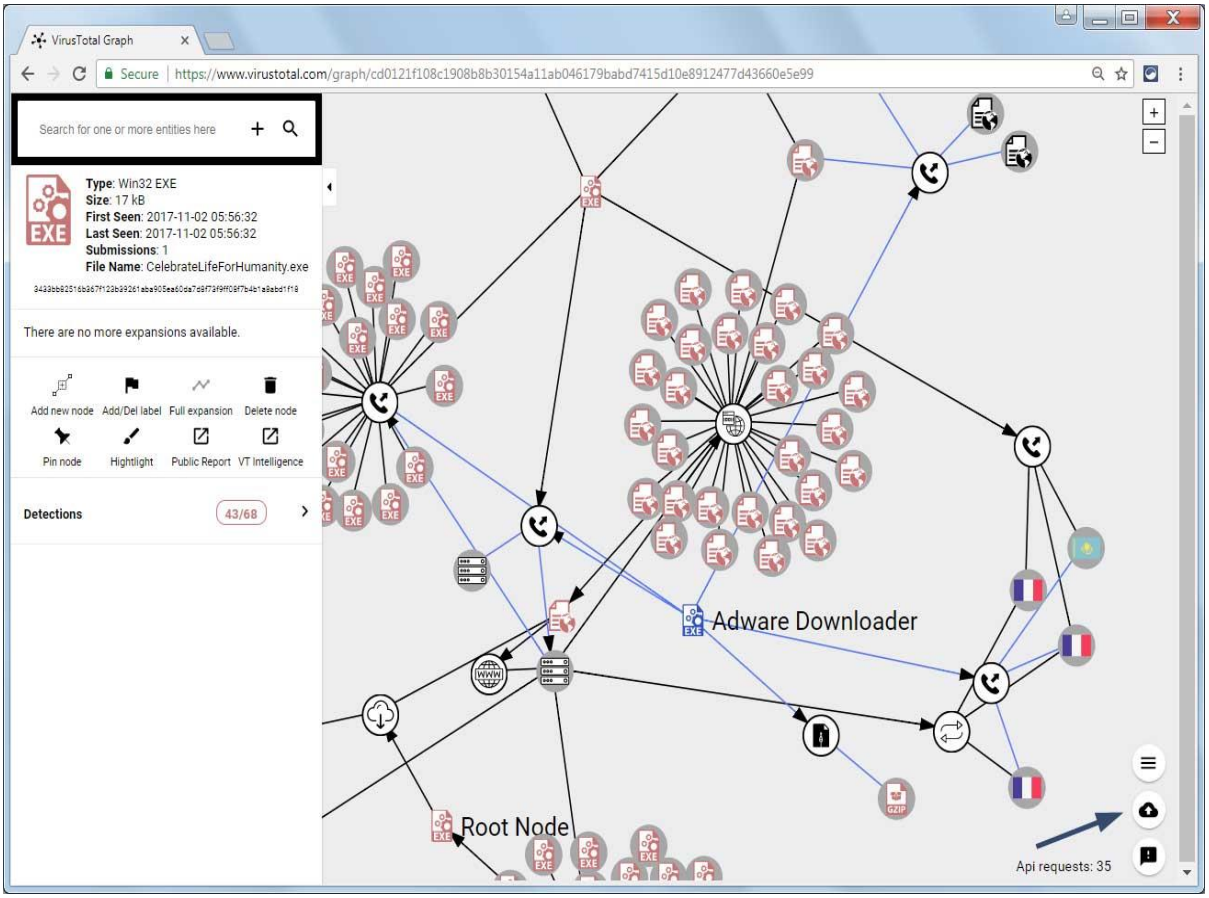



**شکل ۳ گرافی که فایل دانلودشده توسط Root Node را نشان می‌دهد**

بر روی فایل دانلودشده نیز می‌توان دوبارکلیک کرد و اطلاعات مربوط به آن فایل خاص را یافت. این امر به کاربر اجازه می‌دهد تا نمونه‌ای را کاوش کند و تمامی داده‌ها، فایل‌ها، دامنه‌ها، کشورهای مرتبط و URLهایی را که با فایل ارایه‌شده در ارتباط هستند، ببیند.

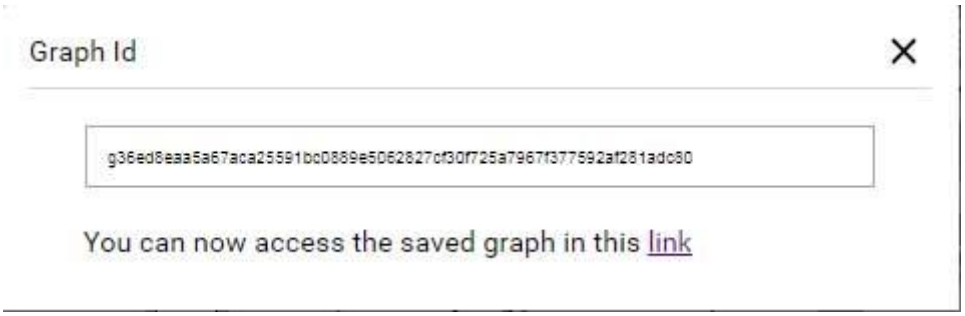
ازآنجایی‌که هرکس می‌تواند گراف پایه‌ی مرتبط به یک فایل را ببیند، امکان سفارشی‌سازی یک گراف خاص و ذخیره‌ی آن برای استفاده شخصی نیز وجود دارد. برای مثال، اگر کاربر در حال تجزیه‌وتحلیل یک نمونه بدافزار خاص باشد و بخواهد برچسب‌هایی را به اشیای مختلف برای زمان جستجو اضافه نماید، به‌راحتی می‌تواند این کار را انجام دهد.

برای اضافه‌کردن برچسب، تنها کافیست کاربر بر روی یک شئ کلیک‌راست کند و برچسبی اضافه نماید. در شکل ۴ برچسب Adware Downloade به شئ فایلی خاص اضافه شده است.




**شکل ۴ برچسب شئ**

همان‌طور که در شکل ۴ با پیکان نشان داده شده است، می‌توان با کلیک بر روی دکمه‌ی ذخیره‌سازی، تنظیمات را در گراف جدید ذخیره کرد. هنگامی‌که یک گراف ذخیره می‌شود، به کاربر لینک جدیدی داده می‌شود تا در آینده بتواند به آن دسترسی داشته باشد یا آن را با دیگران به اشتراک بگذارد (شکل ۵).




**شکل ۵ گراف ذخیره‌شده**

این ابزار که تاکنون بازخورد خوبی دریافت کرده است و از سال گذشته درحال‌توسعه است، برای تجزیه‌وتحلیل بدافزار و موارد مرتبط با آن بسیار مفید خواهد بود.